ETSI TR 133 926 V17.8.0 (2023-10)

TECHNICAL REPORT

LTE;
5G;
Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
(3GPP TR 33.926 version 17.8.0 Release 17)

Reference

RTR/TSGS-0333926vh80

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/CommiteeSupportStaff.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 2023.
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.

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.

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.

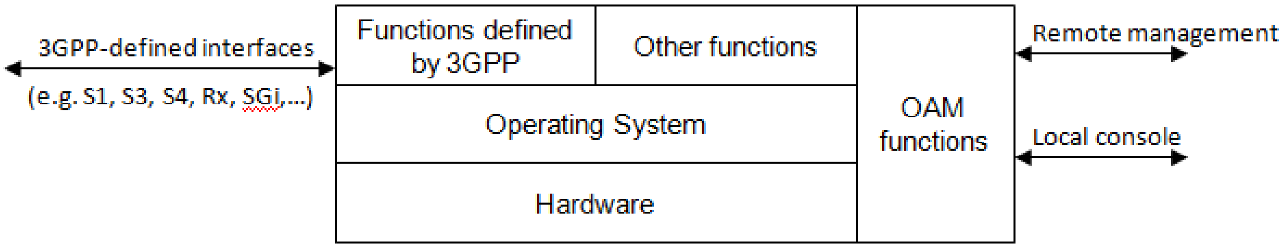

Figure 4.3-1: GNP model

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.

4.4.2 Scope regarding GNP functions defined by 3GPP

The set of GNP functions actually implemented in an GNP is to be described in the annex of the present document. But the GNP SCAS needs to explicitly address all GNP functions that, if present in an GNP network product, need to be evaluated and hence covered by requirements in the GNP SCAS. Furthermore, it is to be avoided that a particular version of an GNP SCAS becomes a moving target. This leads to the following note:

NOTE: Although the present document intends to cover the security problems and security requirements for all NP functions described in 3GPP , what other NP, in additional to the MME, are to be covered is at the discretion of the working group.

4.4.3 Scope regarding other functions

At least the following functions not defined by 3GPP are in scope of the GNP SCAS:

- Remote management functions
- Local management functions

4.4.4 Scope regarding Operating System (OS)

The GNP SCAS does not attempt a full evaluation of the correct internal functioning of the OS. However, interfaces (I.e. the restriction on open ports and unnecessary services running in the system) and modifications (e.g. verification of the correct applied patch level, hardening, etc.) of the OS are in scope.

4.4.5 Scope regarding hardware

The GNP SCAS does not attempt a full evaluation of the correct internal functioning of the hardware platform. However, interfaces that are implemented in hardware (e.g. USB port) and modifications of the hardware are in scope.

4.4.6 Scope regarding interfaces

The interfaces listed in clause 4.3.6 are all in scope of the present document.

5 Generic assets and threats

5.1 Introduction

The present subclause contains assets and threats that are believed to apply to more than one network product.

5.2 Generic critical assets

The critical assets of GNP to be protected are:

- User account data and credentials (e.g. passwords);
- Log data;
- Configuration data, e.g. GNP's IP address, ports, VPN ID, Management Objects (e.g. user group, command group) etc.
- Operating System (OS), i.e. the files that make up the OS and its processes (code and data);
- GNP Application;
- Sufficient processing capacity: that processing powers are not consumed close to limits;
- Hardware, e.g. mainframe, board, power supply unit etc.

- The interfaces of GNP to be protected and which are within SECAM scope: for example
  - Console interface, for local access: local interface on MME
  - OAM interface, for remote access: interface between MME and OAM system

NOTE 1: The detailed interfaces of the GNP are described in clause 4, Generic Network Product Class Description of the present document.

- GNP Software: binary code or executable code

NOTE 2: GNP 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, GNP applications or GNP Software.

5.3 Generic threats

5.3.0 Generic threats format

Threats are described using the following format:

- *Threat Name*:
- *Threat Category*:
- *Threat Description*:
- *Threatened Asset*:

5.3.1 Introduction

Threat analysis is an important step in the SCAS methodology in order to justify a proposed requirement and ensuring that no relevant requirements have been forgotten.

In particular, to ensure this latter point, the threat analysis needs to be free of gaps and overlapping, and it needs to be ensured that all relevant threats are covered by a requirement.

To resolve the overlapping, it is suggested to first look at the action used to exploit the threat being considered. For example if passwords are stored locally in the GNP (e.g. in a database or file system) in an insecure way (e.g. clear text, unsalted hashes), an attacker can retrieve these passwords (e.g. can retrieve the file containing them and can retrieved them by means of brute forcing if unsalted hashes are used) and later use them. So the threat related to this scenario is Information Disclosure.

To achieve this goal, the identified threats are grouped into the seven categories, one covering threats relating to 3GPP-defined interfaces and the other six ones corresponding to the categories proposed by STRIDE [http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx] and reported below:

- **Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
- **Tampering with data**. Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.
- **Repudiation**. Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise. For example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.
- **Information disclosure**. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it. For example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

- **Denial of service**. Denial of service (DoS) attacks deny service to valid users-for example, by making a Web server temporarily unavailable or unusable. You need to protect against certain types of DoS threats simply to improve system availability and reliability.

- **Elevation of privilege**. In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

All the reported threats follow the below template:

- Threat Name: i.e. The name of the threat

- Threat Category: i.e. of the six STRIDE categories

- Threat Description: i.e. description of how the threat can be exploited and eventually the impacts/consequences of its exploitation

- Threatened Asset: e.g. which asset is affected by the threat

5.3.2 Threats relating to 3GPP-defined interfaces

The threats relating to 3GPP-defined interfaces, cf. clause 4.3.6, may have been sufficiently covered, explicitly or implicitly, in the course of the work on 3GPP security specifications. There is no need to repeat this work for the purposes of the present SCAS, and these threats and risks are therefore not considered here separately.

NOTE: Not all threats and risks covered by security mechanisms in existing 3GPP security specifications may have been adequately documented in a 3GPP TS or TR.
They may have also been addressed in contributions to 3GPP Working Group meetings.
A good source for these threats and risks is 3GPP TR 33.821 [4].
Note also that threats that relate to actions local to the NP and/or do not affect interoperability may also not have been addressed by existing 3GPP work.

When threats relating to 3GPP-defined interfaces are found that are not sufficiently covered in existing 3GPP security specifications, they need to be addressed in the present SCAS. Generic threats, e.g. threats relating to protocol robustness, that also apply to 3GPP-defined interfaces are covered in the present clause.

5.3.3 Spoofing identity

5.3.3.1 Default Accounts

- *Threat name:* Default Accounts

- *Threat Category*: Spoofing Identity

- *Threat Description*: A default account with a default password or just a user account with a default password may be provided on GNP and this password may not be modified in time. An attacker can get this password, for example, for low clearance level user, even high clearance level user from document or by brute forcing. With the default password an attacker can access to the GNP, via console (e.g. via direct connection to the GNP via serial and/or usb ports) or via network interfaces (e.g. management and maintenance), and modify, for example, the configuration and/or interference of the normal network operation.

- *Threatened Asset*: User account data and credentials

5.3.3.2 Weak Password Policies

- *Threat name:* Weak Password Policies

- *Threat Category:* Spoofing Identity

- *Threat Description:* Weak password policies (e.g. short password length, blank passwords, password age, historical passwords and password dictionary) can make a password cracking very simple (e.g. in a short time the password can be guessed by brute forcing). With these passwords an attacker can access to the GNP, via console (e.g. via direct connection to the GNP via serial and/or usb ports) or via network interfaces (e.g. management and maintenance), and modify, for example, the configuration and/or interference of the normal network operation.

- *Threatened Asset:* User account data and credentials

5.3.3.3 Password peek

- *Threat name:* Password peek
- *Threat Category:* Spoofing Identity
- *Threat Description:* When password in plain text has been displayed on screen, it can be seen easily by another local observer besides operator. With these passwords an attacker can access to the GNP, via console (e.g. via direct connection to the GNP via serial and/or usb ports) or via network interfaces (e.g. management and maintenance), and modify, for example, the configuration and/or interference of the normal network operation.
- *Threatened Asset:* User account data and credentials

5.3.3.4 Direct Root Access

- *Threat name:* Direct Root Access
- *Threat Category:* Spoofing Identity
- *Threat Description:* An attacker fraudulently access directly to the root account via the network/remote connection, for example by brute forcing attack.
- *Threatened Asset:* all critical assets of GNP as listed in clause 5.2, except hardware assets

5.3.3.5 IP Spoofing

- *Threat Name:* IP Spoofing
- *Threat Category:* Spoofing Identity.
- *Threat Description:* IP spoofing is used to gain unauthorized access to a computer. An attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system.
- *Threatened Asset:* GNP.

5.3.3.6 Malware

- *Threat Name:* Malware
- *Threat Category:* Spoofing Identity, Denial of Service, Elevation of Privilege, Tampering, Information Disclosure
- *Threat Description:* A malware can act as a legitimate user and perform malicious activities.
- *Threatened Asset:* all critical assets of GNP as listed in clause 5.2, except hardware assets

5.3.3.7 Eavesdropping

Threat name: Eavesdropping

Threat Category: Spoofing Identity, tampering, repudiation

- *Threat Description*: Eavesdropping or sniffing is an attack consisting of capturing network traffic and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information. So, an attacker can eavesdrop network traffic, for example, on the management/maintenance interfaces to retrieve credentials which can be used to spoof user identity. Eavesdropping can be performed, e.g. by means of MITM attacks. This type of attacks may be possible, for example, if weak cryptographic protocols or non-industry standard cryptographic algorithms are used or if the communication protocols have been implemented incorrectly.

- *Threatened Asset*: User account data and credentials

5.3.4 Tampering

5.3.4.1 Software Tampering

- *Threat Name*: Software Tampering
- *Threat Category*: Tampering
- *Threat Description*: Software packages can be tampered/altered during their installation/upgrade on the GNP. An attacker, for example, can inject malicious code, altering their legitimate behaviour. After their installation or upgrade process, the malicious code can be executed to conduct several attacks (e.g. DoS, Information Stealing, Frauds and so on).
- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, including hardware assets.

5.3.4.2 Ownership File Misuse

- *Threat Name*: Ownership File Misuse
- *Threat Category*: Tampering
- *Threat Description*: If files owned by an user (root user as well as not root users) can be altered improperly and illegitimately by an user different than the owner, then an attacker can conduct several types of attacks (e.g. DoS, Information Stealing, and so on)
- *Threatened Asset*: GNP files.

5.3.4.3 External Device Boot

- *Threat name*: External Device Boot
- *Threat Category*: Tampering
- -*Threat Description:* If GNP operating system can be booted not only from internal memory but also from another source (e.g. USB flash drive, memory card), the GNP bootloader may maliciously be tampered by an attacker. This does not necessarily mean that booting from external memories constitutes a threat.
- *Threatened Asset:* hardware, operating system

5.3.4.4 Log Tampering

- *Threat name*: Log Tampering
- *Threat Category*: Tampering, Repudiation
- *Threat Description:* if GNP does not securely store log files, an attacker, for example can inject, delete or otherwise tamper with the contents of the logs typically for the purposes of masking other malicious behavior.
- Threatened Asset: Log file

5.3.4.5 OAM Traffic Tampering

- *Threat name*: OAM Traffic Tampering
- *Threat Category*: Tampering

- *Threat Description:* Usage of weak cryptographic algorithms for transmitted sensitive information/data over OAM interface can expose them to be maliciously tampered. For example an attacker can gain access to the management /maintenance interfaces and can modify the data stream to/from the GNP.

- *Threatened Asset:* sensitive data transferred over OAM

5.3.4.6 File Write Permissions Abuse

- *Threat name*: File/Directory Write Permissions Misuse

- *Threat Category*: Tampering

- *Threat Description*: File write permissions which are far too liberal are potentially vulnerable and can be abused by an attacker to cause DoS. For example file passwords permissions with write permissions too liberal can be altered by an unauthorized user which can change the administration password, causing the impossibility for the administrator to log on the GNP.

- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, except hardware assets.

5.3.4.7 User Session Tampering

- *Threat name*: User Session Tampering

- *Threat Category*: Tampering

- *Threat Description:* Usage of insufficiently random values used to identify an user session (e.g. sessionID for web sessions) can be exploited by an attacker to tamper this user session by predicting/guessing these identifiers.

- *Threatened Asset:* User Sessions

5.3.5 Repudiation

5.3.5.1 Lack of User Activity Trace

- *Threat Name:* Lack of User Activity Trace

- *Threat Category:* Repudiation

- *Threat Description:* A system user, including a possible attacker, can maliciously or erroneously access and modify data in the GNP system, with no or lesser possibility of the actions later being traceable to his/her user identity. One scenario of anonymity is when the user is logged on to a system group account.

- *Threatened Asset:* all critical assets of GNP as listed in clause 5.2, except hardware assets

5.3.6 Information disclosure

5.3.6.1 Poor key generation

- *Threat Name*: Poor key generation

- *Threat Category*: Information Disclosure

- *Threat Description*: A poor key generation may help an attacker to discover and disclose the key and then read or modify the encrypted data. Attackers can discover a key, for example, if:

  - It was generated in a non-random fashion (e.g. insecure random generator).

  - It was generated starting from a passphrase containing low entropy.

  - The generated key length is too short so the time to retrieve the key by means of dictionary attacks is short.

- *Threatened Asset*: all critical asset in the GNP as listed in clause 5.2 except hardware assets.

5.3.6.2 Poor key management

- *Threat Name*: Poor key management
- *Threat Category*: Information Disclosure
- *Threat Description*: A poor key management may help an attacker to discover the key and then read or modify the encrypted data. Attackers can discover the keys if, for example:
  - Weak key management protocols are used;
  - The keys are stored in an unencrypted file accessible by everyone;
  - The keys are not renewed/updated regularly;
  - The keys which are text strings can be found by looking for all strings in the system;
  - The keys can be found in memory image of running processes;
  - RAM does not loose contents immediately after power-down;
  - RAM can be investigated for keys;
  - The keys are not safely destroyed after their use.
- *Threatened Asset*: all critical asset in the GNP as listed in clause 5.2 except hardware assets.

5.3.6.3 Weak cryptographic algorithms

- *Threat Name*: Use of weak cryptographic algorithms
- *Threat Category*: Information Disclosure
- *Threat Description*: Usage of weak cryptographic algorithms for stored or transmitted sensitive information/data can expose them to be disclosed and eventually tampered.
- *Threatened Asset*: all critical asset in the GNP as listed in clause 5.2 except hardware assets.

5.3.6.4 Insecure Data Storage

- *Threat name*: Insecure Data Storage
- *Threat Category*: Information Disclosure
- *Threat Description:* GNP stores locally sensitive data (e.g. communication keys (i.e. K_{NASenc}, K_{NASint}, K_{eNB}), passwords). An attacker can retrieve these data if they have been stored in an insecure way (e.g. clear text, unsalted hashes).
- *Threatened Asset*: Any sensitive data stored locally to the GNP

5.3.6.5 System Fingerprinting

- *Threat Name*: System Fingerprinting
- *Threat Category*: Information Disclosure
- *Threat Description*: The GNP could potentially disclose information about account details, operating system version and/or other software versions, server names and so on. That can be used by an attacker to perform other attacks.
- *Threatened Asset*: all critical asset in the GNP as listed in clause 5.2 except hardware assets.

5.3.6.6 Malware

- *Threat Name*: Malware.

- *Threat Category*: Information Disclosure.
- *Threat Description*: A malware installed on GNP can access to all the sensitive data stored locally to the GNP (e.g. accounts, keys, and user data).
- *Threatened Asset*: all critical asset in the GNP as listed in clause 5.2 except hardware assets.

5.3.6.7 Personal Identification Information Violation

- *Threat Name:* Personal Identification Information Violation.
- *Threat Category*: Information Disclosure.
- *Threat Description*: Data containing identities of mobile network subscribers are critical for user privacy. Leakage of these user's identities can lead to loss of privacy, e.g. tracing of a user. Protection of user's identities is also a requirement from regulators.
- *Threatened Asset*: Mobility Management data (e.g. user identities).

5.3.6.8 Insecure Default Configuration

- *Threat Name:* Insecure Default Configuration
- *Threat Category*: Information Disclosure
- *Threat Description*: An attacker could exploit an insecure default GNP configuration and access to sensitive information/data available on the GNP.

For example a default GNP can use NULL integrity not only for unauthenticated emergency calls. This can compromise the integrity of RRC signalling and make possible Man in the Middle attacks in the AS domain and interception, for example, of user communications.

- *Threatened Asset*: GNP configuration data and mobility management data.

5.3.6.9 File/Directory Read Permissions Misuse

- *Threat name*: File/Directory Read Permissions Misuse
- *Threat Category*: Information Disclosure, elevation of privilege, DoS, tampering
- *Threat Description*: File and directory read permissions which are far too liberal can allow access to the contained data by illegitimate users (e.g. password files with too liberal file permissions can be accessed by unauthorized users).
- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, except hardware assets

5.3.6.10 Insecure Network Services

- *Threat name*: Insecure Network Services
- *Threat Category*: Information Disclosure
- *Threat Description*: The GNP can expose insecure/vulnerable services/open ports which can be exploited by an attacker to gain sensitive information/data. For example the GNP can be configured to return sensitive information using telnet on a custom port without any authentication mechanism being configured.
- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, except hardware assets

5.3.6.11 Unnecessary Services

- *Threat name*: Unnecessary Services
- *Threat Category*: Information Disclosure

- *Threat Description*: The GNP can expose unnecessary services which can be exploited (even if not vulnerable) by an attacker to gain sensitive information/data.

The term unnecessary used in this threat refers to three cases:

  - Network service not strictly related to GNP operation (e.g. Splunk Service)
  - Network service available on unexpected interfaces (e.g. SSH enabled on the interface interconnecting GNP and Remote Management)
  - Service that does not enable a network service but that runs on the GNP and is not necessary by GNP normal operation (e.g. fprint service available in the default fedora distribution or Xinetd services).

- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, except hardware assets

5.3.6.12 Log Disclosure

- *Threat name*: Log Disclosure
- *Threat Category*: Information Disclosure
- *Threat Description*: When operational activities are recorded by GNP, these operation records are called system logs. There are other logs, e.g. operation log, security log. These logs can contain sensitive information/data (e.g. system data, user data, CDR, or also debugging information) which can be accessed by an attacker to gather information about the system and to perform other attacks towards users or the system itself.
- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, except hardware assets

5.3.6.13 Unnecessary Applications

- *Threat name*: Unnecessary Applications
- *Threat Category*: Information Disclosure
- *Threat Description*: There are applications (i.e. features and functionalities) in the GNP which can be related to personal privacy (e.g. LCS application). Even if an operator does not deploy these features and functionalities, they can be available in the system as part of a software distribution. Consequently there might be the risk that an attacker enables these applications without authorization (e.g. despite of what is included in the license issued by the vendor). For example, the attacker may enable a feature such as LCS and get the location information of a user.
- *Threatened Asset*: personal privacy related features, functions and applications, e.g. LCS.

5.3.6.14 Eavesdropping

- *Threat name*: Eavesdropping
- *Threat Category*: Information Disclosure
- *Threat Description*: An attacker can eavesdrop network traffic, for example, on the management/maintenance interfaces. This may be possible if weak cryptographic protocols or non-industry standard cryptographic algorithms are used or if the communication protocols are implemented incorrectly. Eavesdropping can be performed, for example, by means of MITM attacks, Arp Poisoning, ICMP Redirect and so on.
- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2

5.3.6.15 Security threat caused by lack of GNP traffic isolation

- *Threat name*: Security threat caused by lack of GNP traffic isolation
- *Threat Category*: Information disclosure
- *Threat Description:* The attack towards signalling traffic can also impact the management traffic and vice versa when these traffics are not isolated. For example, an attacker wants to obtain important information related to

signalling, he can intercept and capture signalling traffic on GNP's interface. The important information related management may also be intercepted and captured if the management traffics and signalling traffics are not isolated and use the same physical interface. So the security threats for signalling traffic can impact management traffic and result in unauthorized access on GNP. In the same way, an attacker who attacks GNP's management traffics can obtain important information related signalling, resulting in tampering and privacy leakage of signalling.

- *Threatened Asset:* all critical data transferred via the GNP as listed in clause 5.2

5.3.7 Denial of service

5.3.7.1 Compromised/Misbehaving User Equipments

- *Threat Name*: Compromised/Misbehaving User Equipments
- *Threat Category*: DoS
- *Threat Description*: A large number of compromised or misbehaving user equipments (UE) can cause a fault on the GNP with a consequent denial of service.

For example, an attacker can control a huge number of UEs and can send a lot of contemporary attach/detach requests to the GNP without following the normal protocol flow. The resources on the GNP (e.g. processing resources or radio resources) can be exhausted and the GNP becomes unable to process other, valid NAS signalling requests.

- *Threatened Asset*: GNP resources (e.g. system processing capacity (e.g. CPU, memory), network links, radio links and so on).

5.3.7.2 Implementation Flaw

- *Threat Name*: Implementation Flaw.
- *Threat Category*: DoS.
- *Threat Description*: An attacker can exploit an implementation flaw in one of the protocols supported by a GNP or in one application available on the GNP and cause a DoS.
- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, except hardware assets.

5.3.7.3 Insecure Network Services

- *Threat name*: Insecure Network Services.
- *Threat Category*: DoS.
- *Threat Description*: The GNP can expose insecure/vulnerable services/open ports which can be exploited by an attacker to crash the GNP.
- *Threatened Asset*: GNP services.

5.3.7.4 Human Error

- *Threat name:* Human Error
- *Threat Category*: Denial of service
- *Threat Description*: The general threat of human error in operation and maintenance. This can include network-, network element-, and firewall configuration-settings. It can also include the risk of user accounts being forgotten during change or deletion, or other slips in their handlings. Causes can be maintenance workload, fatigue, inexperience, etc., and may arise irrespective of applied policy. This threat, for network operation, is hard to categorize within the STRIDE approach, but with Denial of service being one important threat category.

- *Threatened Asset*: all critical assets of GNP as listed in clause 5.2, except hardware assets.

5.3.8 Elevation of privilege

5.3.8.1 Misuse by authorized users

- *Threat Name*: misuse by authorized users
- *Threat Category*: Elevation of Privilege
- *Threat Description*: A malicious employee or his/her co-worker misuses the network access and management authorization to attempts to upgrade his/her account to, for example, administrative privileges or to gain access to password files within the system.
- *Threatened Asset*: The network access and management authorization.

5.3.8.2 Over-Privileged Processes/Services

- *Threat Name*: Over-Privileged Processes/Services.
- *Threat Category*: Elevation of Privilege.
- *Threat Description*: GNP processes/services running with higher privileges than needed, (i.e. root or Administrator) can allow an attacker to obtain elevated privileges as well. An attacker can for example try to leverage a bug in the running program and execute arbitrary code with elevated privileges.

. *Threatened Asset*: Over-Privileged Processes/Services.

5.3.8.3 Folder Write Permission Abuse

- *Threat Name:* Folder Write Permission Abuse
- *Threat Category*: Elevation of Privilege
- *Threat Description*: weaknesses in folder permissions can lead to elevation of privilege. A root user by mistake can accidentally execute malicious files placed into a directory by attackers which have sufficient write permissions. The same applies for other directories where users other than root have write permission. Any account that has folder permission on a directory has equivalent access to the executable file within that directory. These permissions allow a non-administrator to replace directories containing executable files with new directories containing new executable files or simply to delete directories and the executable files they contain.
- *Threatened Asset*: System folders with weak write permission.

5.3.8.4 Root-Owned File Write Permission Abuse

- *Threat Name*: Root-Owned File Write Permission Abuse.
- *Threat Category*: Elevation of Privilege.
- *Threat Description*. Failure to protect root-owned executables files from write access by non-administrators exposes them to the possibility of being compromised. For example, this means that non-administrator users can replace or alter the file's contents and that unknown or malicious injected code can then be executed inadvertently by root.
- *Threatened Asset*: Root-Owned Files with weak write permission.

5.3.8.5 High-Privileged Files

- *Threat name:* High-privileged files.
- *Threat Category:* Elevation of Privilege, DoS, tampering.

- *Threat Description:* If files can be run with higher privileges that what the owner normally has, i.e. with temporarily elevated rights, it can be dangerous to system.
- *Threatened Asset:* High privileged files.

5.3.8.6 Insecure Network Services

- *Threat name*: Insecure Network Services.
- *Threat Category*: Elevation of Privilege.
- *Threat Description*: The GNP can expose insecure/vulnerable services/open ports which can be exploited by an attacker to gain unauthorized access, for example using telnet on a custom port without any authentication mechanism configured.
- *Threatened Asset:* Insecure network services/ports.

5.3.8.7 Elevation of Privilege via Unnecessary Network Services

- *Threat name*: Unnecessary Network Services
- *Threat category*: Elevation of Privilege, Denial of Service
- *Threat Description*: The GNP can expose unnecessary services/open ports which can be exploited by an attacker to gain unauthorized access thus leading to elevation of privilege. The term unnecessary used in this threat refers to two cases:
  - Network services not strictly related to GNP operation (e.g. Splunk Service)
  - Network service available on unexpected interfaces (eg. SSH enabled on the interface interconnecting GNP and Remote Management)
- *Threatened Asset:* all critical assets of GNP as listed in clause 5.2, except hardware assets.

6 Generic assets and threats for network functions supporting SBA interfaces

6.1 Introduction

In addition to the assets and threats described in clause 5 for GNP, the present clause contains assets and threats that are believed to apply to all network functions supporting service based interfaces.

6.2 Generic critical assets

The generic critical assets of NF to be protected are:

- NF Application.
- NF API data (e.g. API message IEs, access tokens, client credentials assertions).

Editor's Note: A formulation for indicating the applicable release for the critical assets is needed.

- The interfaces of NF to be protected and which are within SECAM scope:
  - Service Based Interfaces.

6.3 Generic threats

6.3.1 Introduction

The threats described in this subclause follow the template in clause 5. Related security requirements and test cases have been captured in TS 33.117 [17].

6.3.2 Threats related to Service Based Interfaces

6.3.2.1 JSON Parser Exploits

- *Threat Name*: JSON Parser Exploits
- *Threat Category*: Tampering, Information Disclosure, Denial of Service
- *Threat Description*: one of the JSON parser exploits is that the parsers used by a generic NF may execute JavaScript or any other code contained in JSON objects received on SBIs, which are considered untrusted. Further, these parsers may include resources external to the received JSON object itself, such as files from the NF's filesystem or other resources loaded externally. With such exploit, malicious code can be executed by an attacker to conduct several attacks e.g. tampering, information disclosure/stealing, DoS.
- *Threatened Asset*: all critical assets as listed in clauses 5.2 and X.2, except hardware assets

6.3.2.2 JSON Parser not Robust

- *Threat Name*: JSON Parser not Robust.
- *Threat Category*: Denial of Service.
- *Threat Description*: there are following threats if JSON parsers are not robust:
    - For data structures where values are accessible using names (sometimes referred to as keys), e.g. a JSON object, if the names/keys are not unique and duplicated names/keys occur within such a structure, it can result in inconsistent values for that names (or keys), which leads to Denial of Service.
    - If the format and range of values for the IEs in API messages are not implemented as required (e.g. when the number of leaf IEs exceeds the maximum number or when the size of the JSON body of any HTTP request exceed the maximum size), security vulnerabilities may be introduced such as buffer overflow flow, which may lead to Denial of Service.
- *Threatened Asset*: NF API data, NF Application, Sufficient Processing Capability.

6.3.3 Threats related to service access

6.3.3.1 Elevation of privilege via incorrect verification of access tokens

- *Threat name*: Incorrect Verification of Access Tokens.
- *Threat category*: Elevation of Privilege, Information Disclosure, Denial of Service.
- *Threat Description*: there are following threats if the generic NF cannot correctly verify the access tokens:
    - An access token may be tampered so that an attacker can arbitrarily access any services from any NF service providers within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.
    - An access token may be tampered so that an attacker can arbitrarily access the services of any slices provided by the NF producer instances (excluded from the list of NSSAIs or the list NSI IDs) within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.

  - An access token may be tampered so that an attacker can arbitrarily access the services provided by the NF producer instances outside the NF Set which it is allowed to access within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.
  - An access token may be tampered so that an attacker can arbitrarily access the disallowed resources or conduct disallowed actions on the resources for the services provided by a NF service provider within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure.
  - An access token may be tampered so that an attacker can block service access by replacing the granted services/NF service providers with unavailable services/NF service providers, which leads to denial of service.
  - An expired access token can be replayed so that an attack can access the services which may no longer be allowed by the NF service provider, which leads to elevation of privilege and consequently information disclosure.
- *Threatened Asset:* NF API data, NF Application, Sufficient processing capacity.

6.3.4 Threats related to authentication for indirect communication

6.3.4.1 Incorrect validation of client credentials assertion

- *Threat name*: Incorrect Validation of Client Credentials Assertion.
- *Threat category*: Spoofing Identity, Information Disclosure, Denial of Service, Elevation of Privilege.
- *Threat Description*: for indirect communication where NF service consumer and NRF/NF service producer cannot mutually authenticate each other, the authentication of NF service consumer towards NRF/NF service producer can only implicitly rely on authentication between NF service consumer and SCP and between SCP and NRF/NF service producer with hop-by-hop security protection. An additional authentication for indirect communication is using client credentials assertions signed by NF service consumer and validated by NRF/NF service producer, as defined in TS 33.501 [26] clause 13.3.8. Client credentials assertions are sent end-to-end from NF service consumer to NRF/NF service producer via one or several SCPs. There are following threats if the generic NF (including all typers of NF service producer, NRF) receiving the assertion cannot correctly validate it:
  - If the NF could not verify the integrity of the assertion, an attacker can deceive the NF by tampering the instance ID of the consumer NF, audience claim, timestamp and expiration time in the client credentials assertion. This can lead to spoofing identity, information disclosure, denial of service, elevation of privilege.
  - If the NF could successfully verify the integrity of the client credentials assertion but could not verify the audience claim in the assertion, an attacker can deceive the NF with an assertion detined for another NF type intercepted from the consumer NF. This can lead to spoofing identity, information disclosure, elevation of privilege.
  - If the NF could successfully verify the integrity and audience claim of the client credentials assertion but could not verify the expiration time (exp) in the assertion, it can be replayed by an attack, who can abuse the use of assertion for authentication out of its lifetime. This can lead to spoofing identity, information disclosure.
- *Threatened Asset:* NF API data, NF Application, Sufficient processing capacity.

Annex A: Aspects specific to the network product class MME

A.1 Network product class description for the MME

A.1.1 Introduction

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.

A.1.2 Minimum set of functions defining the MME network product 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. Therefore, in order to define the MME network product class it is necessary to define the common set of 3GPP-defined functionalities that is constitutive for an MME. As part of the MME network product, it is expected that the MME contains MME application, a set of running processes (typically more than one) executing the software package for the MME functions and OAM functions that are specific to the MME network product model. Functionalities specific to the MME network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.116 [5].

NOTE: For the purposes of the present document, this common set is defined to be the list of functions contained in clause 4.4.2 of 3GPP TS 23.401, Release 8 [3].

A.2 Assets and threats specific to the MME

A.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the MME to be protected are:

- MME Application;
- Mobility Management data: e.g. subscriber's identities (e.g. IMSI), subscriber keys (I.e. K_{NASenc}, K_{NASint}, NH), authentication parameters, address of serving eNB, APN name, data related to mobility management like UE status, UE's IP address, etc., session management like PDN type, QoS and so on, or node selection and routing selection, e.g. IP address of UE related S/P-GW, selected routing connection based on UE's identity, etc.
- The interfaces of MME to be protected and which are within SECAM scope: for example
    - Console interface, for local access: local interface on MME
    - OAM interface, for remote access: interface between MME and OAM system

NOTE 1: The detailed interfaces of the MME class are described in clause 4, Network Product Class Description of the present document.

- MME Software: binary code or executable code

NOTE 2: MME 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, MME application, Mobility Management data or MME Software.

A.2.2 Threats related to AKA procedures

A.2.2.1 Access to 2G

- *Threat name:* Access to 2G
- *Threat Category*: Tampering of Data, Repudiation, Information Disclosure, Denial of Service
- *Threat Description*: If access to 2G is allowed, an attacker can force the system into 2G mode and use smaller key size, weaker algorithm, etc. to make the system easily attacked and/or compromised.
- *Threatened Asset*: User account data and credentials

A.2.2.2 Resynchronization

- *Threat name:* Resynchronization
- *Threat Reference*: Denial of Service
- *Threat Description*: If RAND and AUTS are not included when synchronization fails, the resynchronization procedure does not work correctly. This can result in waste of system resources and deny a legitimate user access to the system.
- *Threatened Asset*: Sufficient Processing Capacity

A.2.2.3 Failed Integrity check of Attach message

- *Threat name:* Failed integrity check of Attach message
- *Threat Category*: Denial of Service
- *Threat Description*: If integrity check of attach message fails, a user identity cannot be verified. This can result in waste of system resources and deny a legitimate user access to the system.
- *Threatened Asset*: Sufficient Processing Capacity

A.2.2.4 Forwarding EPS authentication data to SGSN

- *Threat name:* Forwarding EPS authentication data to SGSN
- *Threat Category*: Denial of Service
- *Threat Description*: If EPS authentication data is forwarded to SGSN, the SGSN is not expecting the data and does not know how to handle this data. This can cause processing error on the SGSN and negatively impact system performance.
- *Threatened Asset*: Sufficient Processing Capacity

A.2.2.5 Forwarding unused EPS authentication data between different security domains

- *Threat name:* Forwarding unused EPS authentication data between different security domains
- *Threat Category*: Denial of Service
- *Threat Description*: If unused EPS authentication data is forwarded between security domains, system resources will be wasted thus requiring HSS to regenerate new EPS authentication data. This can result in waste of system resources for the receiving system to store the data as well as wasting resources in sending the data.
- *Threatened Asset*: Sufficient Processing Capacity

A.2.3 Threats related to security mode command procedure

A.2.3.1 Bidding Down

- *Threat name:* Bidding down
- *Threat Category*: Tampering of Data, Information Disclosure, Denial of Service
- *Threat Description*: If SMC does not include replayed UE security capabilities of the UE, the UE can force the system to reduce the security level by using weaker security algorithms or turning security off, making the system easily attacked and/or compromised.
- *Threatened Asset*: User account data and credentials

A.2.3.2 NAS integrity selection and use

- *Threat name:* NAS integrity selection and use
- *Threat Category*: Tampering of data, Information Disclosure, Denial of Service
- *Threat Description*: If NAS does not use the highest priority algorithm to protect SMC, SMC risks being exposed and/or modified. This can cause the system to turn off security, making the system easily attacked and/or compromised.
- *Threatened Asset*: Sufficient Processing Capacity

A.2.3.3 NAS NULL integrity protection

- *Threat name:* NAS NULL integrity protection
- *Threat Category*: Elevation of Privilege
- *Threat Description*: If NAS NULL integrity protection is not used correctly, an attacker can initiated unauthenticated non-emergency calls.
- *Threatened Asset*: Sufficient Processing Capacity

A.2.3.4 NAS confidentiality protection

- *Threat name:* NAS confidentiality protection
- *Threat Category*: Tampering of Data, Information Disclosure, Denial of Service
- *Threat Description*: If security mode complete message is not confidentiality protected, the MME cannot be certain that the SMC is executed correctly. This can result in waste of system resources and deny a legitimate user access to the system.
- *Threatened Asset*: Sufficient Processing Capacity

A.2.4 Threats related to security in Intra-RAT mobility

A.2.4.1 Bidding down on X2-Handover

- *Threat name:* Bidding down on X2-Handover
- *Threat Category*: Tampering of Data, Information Disclosure
- *Threat Description*: If MME cannot verify EPS security capabilities received from eNB are the same as the UE security capabilities that the MME has stored, the UE may force the system to accept a weaker security

algorithm than the system is allowed forcing the system into a lowered security level making the system easily attacked and/or compromised.

- *Threatened Asset*: User account data and credentials

A.2.4.2 NAS integrity protection algorithm selection in MME change

- *Threat name:* NAS integrity protection algorithm selection in MME change
- *Threat Category*: Tampering of Data, Information Disclosure
- *Threat Description*: If the highest priority NAS integrity protection is not able to be selected by the new MME in MME change, the new MME could end up using a weaker algorithm forcing the system into a lowered security level making the system easily attacked and/or compromised.
- *Threatened Asset*: User account data and credential

A.2.5 Threats related to security in Inter-RAT mobility

A.2.5.1 2G SIM access via idle mode mobility

- *Threat name:* 2G SIM access via idle mode mobility
- *Threat Category*: Tampering of Data, Information Disclosure
- *Threat Description*: If access to 2G is allowed during idle mode mobility, an attacker can force the system into 2G mode and use smaller key size, weaker algorithm, etc. to make the system easily attacked and/or compromised. The attacker can also illegally obtain LTE service via 2G SIM
- *Threatened Asset*: User account data and credentials

A.2.5.2 2G SIM access via handover

- *Threat name:* 2G SIM access via handover
- *Threat Category*: Tampering of Data, Information Disclosure
- *Threat Description*: If access to 2G is allowed during handover, an attacker can force the system into 2G mode and use smaller key size, weaker algorithm, etc. to make the system easily attacked and/or compromised. The attacker can also illegally obtain LTE service via 2G SIM.
- *Threatened Asset*: User account data and credentials

A.2.5.3 2G SIM access via SRVCC

- *Threat name:* 2G SIM access via handover
- *Threat Category*: Tampering of Data, Information Disclosure
- *Threat Description*: If access to 2G is allowed during SRVCC, an attacker can force the system into 2G mode and use smaller key size, weaker algorithm, etc. to make the system easily attacked and/or compromised. The attacker can also illegally obtain LTE service via 2G SIM.
- *Threatened Asset*: User account data and credential

A.2.6 Threats related to release of non-emergency bearer

- *Threat name:* Release of non-emergency bearer.
- *Threat Category*: Denial of Service.

- *Threat Description*: If authentication fails in the MME and the non-emergency bearer is not released, the UE can continue receiving unauthorized call, wasting valuable system resources.

- *Threatened Asset*: Sufficient Processing Capacity.

Annex B: Aspects specific to the network product class PGW

B.1 Network product class description for the PGW

B.1.1 Introduction

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.

B.1.2 Minimum set of functions defining the PGW network product class

As part of the PGW network product, it is expected that the PGW to contain PGW application, a set of running processes (typically more than one) executing the software package for the PGW functions and OAM functions that are specific to the PGW network product model. Functionalities specific to the PGW network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.250 [11].

NOTE: For the purposes of the present document, this common set is defined to be the list of functions contained in clause 4.4.3.3 of 3GPP TS 23.401, Release 8 [3].

B.2 Assets and threats specific to the PGW

B.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the eNB to be protected are:

- PGW Application;
- Session related data: UE network usage and charging data e.g. subscriber's identities (e.g. IMSI), TEID, Charging ID, packet count, etc.
- User plane data;
- The interfaces of PGW to be protected and which are within SCAS scope: for example
    - SGi interface
    - S5/S8 interfaces
    - Console interface, for local access: local interface on PGW
    - OAM interface, for remote access: interface between PGW and OAM system

NOTE 1: The detailed interfaces of the PGW class are described in clause 4, Network Product Class Description of the present document.

- PGW Software: binary code or executable code

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

B.2.2 Threats related to IP Address Allocation

B.2.2.1 IP Address Reallocation Continuously

- *Threat name:* IP Address Reallocation Continuously
- *Threat Category*: Tampering
- *Threat Description*: If an IP address is reallocated to a UE immediately after released from another UE, then the network side might be mistaken that the same UE keeps using the IP address continuously. Consequently, some network functions (e.g. PCRF) will execute policies on the wrong target UE. And some mis-operations (e.g. mischarging) will be executed on UEs.
- *Threatened Asset:* Session related data

B.2.3 Packet Forwarding

B.2.3.1 Sending unauthorized packets to other UEs

- *Threat name:* Sending unauthorized packets to other UEs
- *Threat Category*: Tampering, DoS
- *Threat Description*: If the destination address of uplink packets sent by a UE is another UE in the same PGW, the packets will not pass through the PGW and will be forwarded directly to the target UE. In this case, mutual access between two UEs within the same PGW might be requested. If such access is enabled, an attacker can gain control of a UE to send malicious packets (e.g. fraudulent information, malicious trojans, virus packs, etc.) directly to other UEs without security measures (e.g. firewall) at network side.
- *Threatened Asset:* User plane data

B.2.4 Emergency PDN Connection

B.2.4.1 Inactive Emergency PDN Connection Release

- Threat Name: Prolonged inactive emergency PDN connections
- Threat Category: Denial of Service
- Threat Description: The PGW is expected to release all bearers corresponding to emergency inactive PDN connections after the configured timeout. If emergency bearers of inactive PDN connections are not released, it may lead to system resource exhaustion.
- Threatened Asset: Sufficient Processing Capacity

B.2.5 Threats related to charging relevant data

B.2.5.1 Failure to assign unique TEID or Charging ID for a session

- *Threat name:* Failure to assign unique TEID or Charging ID for a session
- *Threat Category:* Spoofing Identity, Tampering
- *Threat Description:* Both Charging ID and TEID are the identities used for linking the network usage data per UE. If the Charging ID is not unique per IP-CAN session, or the TEID is not unique per GTP tunnel, the charging information for a PDU session would be wrongly correlated, creating charging errors.
- *Threatened Asset:* Session related data

Annex C: Aspects specific to the network product class eNB

C.1 Network product class description for the eNB

C.1.1 Introduction

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.

C.1.2 Minimum set of functions defining the eNB network product class

As part of the eNB network product, it is expected that the eNB contains eNB application, a set of running processes (typically more than one) executing the software package for the eNB functions and OAM functions that are specific to the eNB network product model. Functionalities specific to the eNB network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.216 [20].

NOTE: For the purposes of the present document, this common set is defined to be the list of functions contained in clause 4.1 of TS 36.300, Release 8 [19] and clause 4.4.1 of TS 23.401, Release 8 [3].

C.2 Assets and threats specific to the eNB

C.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the eNB to be protected are:

- eNB Application;
- Mobility Management data: e.g. subscriber's identities (e.g. IMSI), subscriber keys (i.e. K_{UPenc}, K_{RRCenc}, K_{RRCint}, NH), authentication parameters, address of serving gateway, 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 eNB to be protected and which are within SCAS scope: for example
    - S1 interface
    - X2 interface
    - Console interface, for local access: local interface on eNB
    - OAM interface, for remote access: interface between eNB and OAM system

NOTE 1: The detailed interfaces of the eNB class are described in clause 4, Network Product Class Description of the present document.

- eNB Software: binary code or executable code

NOTE 2: eNB 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, eNB application, Mobility Management data or eNB Software.

C.2.2 Threats related to Control plane and User plane

C.2.2.1 Control plane data confidentiality protection

- *Threat name:* Control plane data confidentiality protection

- *Threat Category:* Tampering data, Information Disclosure, Denial of Service, Masquerading attack.

- *Threat Description:* If the eNB does not provide confidentiality protection for control plane packets on the S1/X2 reference points, then the control plane packets sent between eNBs (eg. inter-eNB handover) and from eNB to MME (eg. handover on MME change) can be manipulated and the eNB can be compromised by attackers to prevent service to legitimate users (eg. Handover failure). Moreover, the UE identifiers, security capabilities, the security algorithms and key materials exchanged between eNBs and eNB-MME can be accessed by the attackers leading to huge security breach. There, any active attacker can perform masquerading by making use of the legitimate users' UE identifiers to gain access to the network. This threat scenario assumes that the S1, X2 reference points are not within the security environment

- *Threatened Asset:* User account data and credential

C.2.2.2 Control plane data integrity protection

- *Threat name:* Control plane data integrity protection

- *Threat Category:* Tampering data, Denial of Service

- *Threat Description:* If the eNB does not provide integrity protection for control plane packets on S1/X2 reference points, the control plane packets between eNBs on X2-C and from eNB to MME on S1-MME interface risks being exposed and/or modified. The intruder manipulations on control plane packets will lead to denial of service to legitimate users. This threat scenario assumes that the S1, X2 reference points are not within the security environment

- *Threatened Asset:* Sufficient Processing Capacity

C.2.2.3 User plane data ciphering and deciphering at eNB

- *Threat name:* User plane data ciphering and deciphering at eNB

- *Threat Category:* Tampering data, Information Disclosure, User tracking, Denial of Service, Man-in-the-middle

- *Threat Description:* If the eNB does not cipher and decipher user plane packets between the Uu reference point and the S1/X2 reference points, then the attackers can manipulate and compromise user packets on Uu, X2-U and S1-U interface to launch Denial of Service as well as Man-in-the middle attack. The attackers can gain access to user identifiers, IMSI, serving network identifiers, location information and can perform user tracking. This threat scenario assumes that the S1, X2 reference points are not within the security environment

- *Threatened Asset:* User account data and credential

C.2.2.4 User plane data integrity protection

- *Threat name:* User plane data integrity protection

- *Threat Category:* Tampering data, Denial of Service

- *Threat Description:* If the eNB does not handle integrity protection for user plane packets for the S1/X2 reference points then all the uplink/downlink user plane packets over X2-U and S1-U can be attacked and/or manipulated by intruders to launch Denial of Service attack. This threat scenario assumes that the S1, X2 reference points are not within the security environment

- *Threatened Asset:* Sufficient Processing Capacity.

C.2.3 Threats related to key reuse

C.2.3.1 Key reuse for eavesdropping

- *Threat name:* Key reuse for eavesdropping

- *Threat Category:* Information Disclosure

- *Threat Description:* if the AS keys are not refreshed by the eNB, the key stream reuse is possible. This can result in information disclosure of AS signalling and user plane data. The threat of key stream reuse occurs under the following conditions:

  - when the PDCP COUNT wraps around and is reused with the same Radio Bearer (RB) identity and with the same K_{eNB}, e.g. due to the transfer of large volumes of data.

  - when the PDCP COUNT is reset to 0 but the RB identity and key stay the same (e.g. the successive Radio Bearer establishment uses the same RB identity and keys, or the RB identity is increased after multiple calls and wraps around).

- *Threatened Asset:* User plane data, Mobility Management data.

Annex D: Aspects specific to the network product class gNB

D.1 Network product class description for the gNB

D.1.1 Introduction

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.

D.1.2 Minimum set of functions defining the gNB network product class

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. Related security requirements and test cases have been captured in TS 33.511 [6].

Note: For the purposes of the present document, this common set is defined to be the list of gNB functions contained in TS 38.300 [7], TS 38.323 [9], 3GPP TS 38.322 [10], and TS 23.501 [8].

D.2 Assets and threats specific to the gNB

D.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, 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. K_{UPenc}, K_{UPint}, K_{RRCenc}, K_{RRCint}, 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

NOTE 1: The detailed interfaces of the gNB class are described in clause 4, Network Product Class Description of the present document.

- 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.

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

D.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.

D.2.2.2 Control plane data integrity protection

- *Threat name:* Control plane data integrity protection.

- *Threat Category:* Tampering data, Denial of Service.

- *Threat Description:* If the gNB does not provide integrity protection for control plane packets on N2/Xn/Uu reference points, the control plane packets sent over these reference points can be modified. The intruder manipulations on control plane packets can lead to denial of service to legitimate users. This threat scenario assumes that the N2 and Xn reference points are not within the security environment.

- *Threatened Asset:* Sufficient Processing Capacity, Mobility Management data.

D.2.2.3 User plane data confidentiality protection at gNB

- *Threat name:* User plane data confidentiality protection at gNB.

- *Threat Category:* Information Disclosure.

- *Threat Description:* If the gNB does not cipher and decipher user plane packets on the Uu reference point and the N3/Xn reference points, then the attackers can compromise user packets on Uu, Xn-U, and N3 interface. The attackers can gain access to user identifiers, serving network identifiers, location information and can perform user tracking. This threat scenario assumes that the N3 and Xn reference points are not within the security environment.

- *Threatened Asset:* user plane data.

D.2.2.4 User plane data integrity protection

- *Threat name:* User plane data integrity protection.

- *Threat Category:* Tampering data, Denial of Service.

- *Threat Description:* If the gNB does not handle integrity protection for user plane packets for the Xn reference points then all the uplink/downlink user plane packets over Xn-U can be attacked and/or manipulated by intruders to launch Denial of Service attack. This threat scenario assumes that the Xn reference points are not within the security environment.

- *Threatened Asset:* Sufficient Processing Capacity, User plane data.

D.2.2. 5 AS algorithm selection and use

- *Threat name:* AS algorithm selection and use
- *Threat Category*: Tampering data, Information Disclosure, Denial of Service
- *Threat Description*: If AS does not use the highest priority algorithm to protect AS layer, i.e. RRC and PDCP, data on the AS layer risks being exposed and/or modified, or denial of service.
- *Threatened Asset*: Sufficient Processing Capacity, Mobility Management data

D.2.2.6 Bidding down on Xn-Handover

- *Threat name:* Bidding down on Xn-Handover.
- *Threat Category*: Tampering Data, Information Disclosure, Denial of Service.
- *Threat Description*: If the gNB does not send the UE 5G security capabilities, the AMF cannot verify 5G security capabilities are the same as the UE security capabilities that the AMF has stored, the attacker (e.g gNB) may force the system to accept a weaker security algorithm than the system is allowed, forcing the system into a lowered security level making the system easily attacked and/or compromised.
- *Threatened Asset*: Sufficient processing capability, Mobility Management data.

D.2.2.7 Key Reuse

- *Threat name:* Key Reuse.
- *Threat Category*: Information Disclosure.
  - *Threat Description*: If AS keys are not refreshed by the gNB when PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same K_{gNB}, key stream reuse is possible. This can result in information disclosure of AS signalling and user plane data. The threat of key stream reuse occurs under the following conditions when the PDCP COUNT is reset to 0 but the RB identity and key stay the same (e.g. the successive Radio Bearer establishment uses the same RB identity and keys, or the RB identity is increased after multiple calls and wraps around.
- *Threatened Asset*: User plane data, Mobility Management data.

D.2.2.8 Security Policy Enforcement

- *Threat name:* Security Policy Enforcement.
- *Threat Category*: Tampering data, Information Disclosure.
- *Threat Description*: If gNB does not follow the security based on security policy provided by SMF, this can lead to no security or reduced security provided to the UE user plane, (e.g. not applying integrity protection when it is required to do so), etc.
- *Threatened Asset*: Sufficient Processing Capability, User plane data.

D.2.2.9 State transition from inactive state to connected state

- *Threat name:* State transition from inactive state to connected state
- *Threat Category*: Denial of Service.
- *Threat Description*: When state transits from inactive state to the connected state, if the gNB does not reactivate/activate the UP security based on UP activation status included in the UE 5G AS security context, the UP activation status between the gNB and the UE may be different. This will cause the misalignment on UP

activation status, and result in the UE has to reconnect to the Network again which wastes resource both at UE and gNB.

- *Threatened Asset*: Sufficient Processing Capability.

Annex E: Aspects specific to the network product class UDM

E.1 Network product class description for the UDM

E.1.1 Introduction

This Annex covers the aspects specific to the UDM network product class.

E.1.2 Minimum set of functions defining the UDM network product class

As part of the UDM network product, it is expected that the UDM to contain UDM application, a set of running processes (typically more than one) executing the software package for the UDM functions and OAM functions that is specific to the UDM network product model. Functionalities specific to the UDM network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.514 [21].

NOTE: For the purposes of the present document, this common set is defined to be the list of UDM functions contained in clause 6.2.5 of 3GPP TS 23.501 [8].

E.2 Assets and threats specific to the UDM

E.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the UDM to be protected are:

- UDM Application;
- User Subscription Data: e.g. subscriber's identities (e.g. SUPI), Subscription related data (e.g., Credentials, Access and Mobility Subscription data, SMF Selection Subscription data, UE context in SMF data, authentication status, etc.), etc.
- The interfaces of UDM to be protected and which are within SECAM scope:
  - Service based interface, Nudm, for providing services to AMF, SMF, AUSF, NEF, PCF, GMLC, SMSF
  - Service based interface for consuming services from AMF, AUSF, UDR, NRF.
  - Console interface, for local access: local interface on UDM
  - OAM interface, for remote access: interface between UDM and OAM system

NOTE 1: The detailed interfaces of the UDM class are described in clause 4, Network Product Class Description of the present document.

- UDM Software: binary code or executable code

NOTE 2: UDM 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, UDM application, User Subscription data or UDM Software.

E.2.2 Threats related to UDM assets

E.2.2.1 Incorrect SUCI de-concealment

- *Threat name:* Incorrect SUCI de-concealment

- *Threat Category:* Denial of Service

- *Threat Description:* If the SUPI in the UE and the SUPI retrieved from Nudm_Authentication_Get Response message are not the same, the AMF key generated based on the SUPI in the UE is also not the same as the AMF key generated in the AMF/SEAF. As a result the subsequent NAS SMC procedure will always fail. Hence, UE will never be able to use the services provided by the serving AMF.

- *Threatened Asset:* Sufficient Processing Capacity

E.2.2.2 Synchronization failure

- *Threat name:* Synchronization failure

- *Threat Category:* Denial of Service

- *Threat Description:* If the UDM cannot handle the synchronization failure case during primary authentication, the SQN value stored in the UE and that stored in the UDM will not be synchronized. Hence, the UE will not be able to successfully authenticate with the core network.

- *Threatened Asset:* Sufficient Processing Capacity, User Subscription data

E.2.2.3 Failure to store the authentication status

- *Threat name:* Failure to store of authentication status

- *Threat Category:* Denial of Service

- *Threat Description:* If the UDM does not store the authentication status of a UE, the 5G network cannot support the increased home control, which is useful in preventing certain types of fraud, e.g. fraudulent Nudm_UECM_Registration Request sending a malicious AMF for registering the malicious AMF in UDM that is not actually present in the visited network. Without the authentication status in the UDM, or if the stored authentication status is incorrect, the Nudm_UECM_Registration Request sent from malicious AMF may be accepted.

- *Threatened Asset:* Sufficient Processing Capacity, User Subscription data

E.2.2.4 Incorrect security enforcement configuration

- *Threat name:* Incorrect security enforcement configuration

- *Threat Reference*: Tampering data, Information Disclosure

- *Threat Description*: In case where the UDM is configured to set and provide the User Security Policy to the SMF for TSC service, if the UP security policy is not set to "required", the gPTP message transferred from gNB to a 5GS TSC-enabled UE in the user plane may be removed, tampered or intercepted by an attacker.

E.2.2.5 Incorrect UP security policy configuration for 5G LAN service

- *Threat name:* Incorrect UP security policy configuration for 5G LAN service

- *Threat Reference*: Tampering data, Information Disclosure

- *Threat Description*: It is assumed that two UEs are belonging to one 5G LAN group. In case where the UDM is configured to set and provide User Plane Security policy to the SMF, if the UP security policies set for all the UEs belonging to a specific 5G LAN service are not consistent, e.g. the UP security policy1 for the UE1 is set to "required", and the UP security policy2 for the UE2 is set to "not needed", the 5G LAN service data transferred from gNB to UE2 may be removed, tampered or intercepted by the attacker, even if the service data transferred to the UE1 is protected. That means, the 5G LAN service data will be in the risk of being attacked with the lowest security level set in the the UP security policy.

- *Threatened Asset*: User Subscription Data

Annex F: Aspects specific to the network product class AUSF

F.1 Network product class description for the AUSF

F.1.1 Introduction

This annex captures the aspects specific to network product class AUSF.

F.1.2 Minimum set of functions defining the AUSF network product class

As part of the AUSF network product, it is expected that the AUSF to contain AUSF application, a set of running processes (typically more than one) executing the software package for the AUSF functions and OAM functions that is specific to the AUSF network product model. Functionalities specific to the AUSF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.516 [12].

Note: For the purposes of the present document, this common set is defined to be the list of AUSF functions contained in clause 6.2.8 of 3GPP TS 23.501 [8].

F.2 Assets and threats specific to the AUSF

F.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the AUSF to be protected are:

- AUSF Application;
- User Data: e.g. subscriber's identities (e.g. SUPI), authentication parameters (e.g. Serving network name, authentication vectors, AUSF key), Routing indicator etc.
- The interfaces of AUSF to be protected and which are within SECAM scope:
    - Service based interface, Nausf, for providing services for AMF and UDM
    - Service based interface for consuming services from UDM, and NRF
    - Console interface, for local access: local interface on AUSF
    - OAM interface, for remote access: interface between AUSF and OAM system

NOTE 1: The detailed interfaces of the AUSF class are described in clause 4, Network Product Class Description of the present document.

- AUSF Software: binary code or executable code

NOTE 2: AUSF 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, AUSF application, User data or AUSF Software.

F.2.2 Threats related to authentication procedures

No specific threats are identified for AUSF in addition to the generic threats identified in the main body of this document.

Annex G: Aspects specific to the network product class SEPP

G.1 Network product class description for the SEPP

G.1.1 Introduction

This annex captures the aspects specific to network product class SEPP.

G.1.2 Minimum set of functions defining the SEPP network product 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. Therefore, in order to define the SEPP network product class, it is necessary to define the common set of 3GPP-defined functionalities that is constitutive for a SEPP. As part of the SEPP network product, it is expected that the SEPP contains SEPP application, a set of running processes (typically more than one) executing the software package for the SEPP functions and OAM functions that is specific to the SEPP network product model. Functionalities specific to the SEPP network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.517 [13].

Note: For the purposes of the present document, this common set is defined to be the list of functions contained in clause 6.2.17 of 3GPP TS 23.501 [8].

G.2 Assets and threats specific to the SEPP

G.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the SEPP to be protected are:

- SEPP Application;
- Service Messages to be sent/received over N32.
- SEPP security capability (i.e. N32 protection mechanisms): Mechanism 1 (N32 Application Layer Security), Mechanism 2 (TLS), etc.
- Application layer security data: e.g. N32-f peer information, N32-f security context, cryptographic material of peer SEPPs, cryptographic material of IPX providers, etc.
- Protection policies: e.g. data-type encryption policy and modification policy for outgoing and incoming messages, as described in clause 13.2.3.5 of TS 33.501 [14].
- Internal topology information;
- The interfaces of SEPP to be protected and which are within SECAM scope:
    - N32 (N32-c, N32-f).
    - Interfaces between SEPP and NFs.
    - Console interface, for local access: local interface on SEPP.
    - OAM interface, for remote access: interface between SEPP and OAM system.

NOTE 1: The detailed interfaces of the SEPP network product class are described in clause 4.3.6 of the present document.

- SEPP Software: binary code or executable code

NOTE 2: SEPP files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, SEPP application, supported N32 protection mechanisms, application layer security data, protection policies, internal topology information, or SEPP Software.

G.2.2 Threats related to cryptographic material in the SEPP

G.2.2.1 Misusing cryptographic material of peer SEPPs and IPX providers

- *Threat name:* Misusing cryptographic material of peer SEPPs and IPX providers
- *Threat Category*: Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure
- *Threat Description*: There are following threats if cryptographic material of peer SEPPs and cryptographic material of IPX providers are not clearly differentiated and misused:
  - The SEPP using the wrong cryptographic material will lead to the failure of N32-c TLS connection establishment with the peer SEPP; or lead to rejecting genuine N32-f JSON patches from an authentic intermediate IPX provider. This can result in service interruption as well as waste of system resources.
  - The SEPP will wrongly accept forged N32-f JSON patches signed by a peer SEPP, which maliciously impersonates an intermediate IPX provider. This can result in service data tampering as well as waste of system resources.
  - The SEPP will wrongly establish N32-c TLS connection with an intermediate IPX entity, which maliciously impersonates a peer SEPP. This can result in information disclosure as well as waste of system resources.
- *Threatened Asset*: SEPP Application, N32-c, N32-f, Application layer security data, Sufficient Processing Capacity

G.2.2.2 Misusing cryptographic material beyond connection-specific scope

- *Threat name:* Misusing cryptographic material beyond connection-specific scope
- *Threat Category*: Denial of Service, Tampering of Data, Information Disclosure
- *Threat Description*: There are following threats if the SEPP authenticates N32-f message modifications using the cryptographic material from an IPX provider which was not exchanged as part of the *IPX security information list* via the related N32-c connection:
  - The SEPP using the wrong cryptographic material will lead to failed authentication of N32-f message modifications signed by the authentic IPX provider, who is a part of the related N32-c connection. This can result in service interruption as well as waste of system resources.
  - The SEPP will wrongly accept N32-f JSON patches signed by an IPX provider, who is a part of a different N32-c connection. This can result in service data tampering as well as waste of system resources.
- *Threatened Asset*: SEPP Application, N32-c, N32-f, Sufficient Processing Capacity

G.2.3 Threats related to error handling in the SEPP

G.2.3.1 Incorrect handling for PLMN ID mismatch

- *Threat name:* Incorrect handling for PLMN ID mismatch
- *Threat Category*: Denial of Service, Information Disclosure, Spoofing Identity

- *Threat Description*: there are following threats if the SEPP does not make correct handling when detecting that the PLMN-ID contained in the incoming N32-f message does not match the PLMN-ID in the related N32-f context:
  - Without receiving error signalling message from the SEPP which detected the mismatch, the peer SEPP is not aware of such error and will continue to send the messages with errors. This can result in waste of system resources.
  - If the SEPP sends an error signalling message without indicating the error cause and the corresponding N32-f message ID, the peer SEPP is not able to identify what error occurs and what is the source message on which the error occurs. Hence the peer SEPP is not able to take actions accordingly. This can result in service interruption as well as waste of system resources.
  - The serving PLMN ID appended in the subject claim of the access token sent by a NF service consumer in the serving PLMN will not be checked by the NF service producer in the home PLMN. If the SEPP in the HPLMN detected the mismatch of serving PLMN ID in the access token but still forwards the NF Service Request to the NF service producer, the serving PLMN ID mismatch will not be detected by the NF service producer and the request will be wrongly accepted if all the other checks on the access token get passed. This can result in unauthorized service access by NF service consumer as well as waste of system resources.
- *Threatened Asset*: Application layer security data, Sufficient Processing Capacity

G.2.3.2 Incorrect handling for protection policies mismatch

- *Threat name:* Incorrect handling for protection policies mismatch
- *Threat Category*: Information Disclosure. Tampering of Data, Denial of Service
- *Threat Description*:

For the following threats if the SEPP cannot detect the mismatch between the policies received on N32-c connection from a specific roaming partner and the policies manually configured on it for this specific roaming partner and IPX provider:

  - The policies received on N32-c connection from a peer SEPP could be tampered by an attacker, which is however not detected. Or the policies manually configured on the SEPP could be misconfigured, which is however not detected.
    a) If Data-type encryption policies are tampered or misconfigured, the IEs on N32-f which shall be encrypted may be disclosed due to policy tampering. This can result in information disclosure.
    b) If Modification policies are tampered or misconfigured, the IEs on N32-f which cannot be modified/added/removed by IPX provider may be tampered. This can result in tampering of data.
  - As the data-type encryption policies in the two partner SEPPs are not equal, a consistent ciphering of IEs on N32-f cannot be enforced.
- *Threatened Asset*: Protection policies, SEPP Application, Sufficient Processing Capacity

G.2.4 Threats related to sensitive information exposure

G.2.4.1 Weak JWS algorithm

- *Threat name:* Use of weak JWS algorithm.
- *Threat Category*: Information Disclosure.
- *Threat Description*: There are multiple standard signature algorithms defined for JWS, among which some algorithms may be considered weaker than the others. If an IPX entity is misconfigured, a weak cryptographic algorithm can be used to sign the modifiedDataToIntegrityProtect JSON object, which is more prone to attacks. If the SEPP does not follow the restriction on the signature algorithm for JWS operation as required (using only ES256), it can be exposed to the threat described in clause 5.3.6.3. This can result in sensitive information exposure.

- *Threatened Asset*: SEPP Application.

G.2.4.2 Exposure of confidential IEs in N32-f message

- *Threat name:* Exposure of confidential IEs in N32-f message.
- *Threat Category*: Information Disclosure.
- *Threat Description*: the following behaviours may lead to exposure of confidential IEs in N32-message, which can result in information disclosure:
  - ▪ if the SEPP does not correctly replace the cleartext representations of information elements requiring encryption with the value "encBlockIdx", there is the threat that the sensitive information in original N32-f messages may be exposed to IPX providers in the path or any other parties eavesdropping on the connection between roaming partners.
  - ▪ if the SEPP does not correctly apply the basic validation rule and verify that an intermediate IPX has not inserted an IE requiring encryption at a different location in a JSON object, there is the threat that a misbehaving or compromised intermediate IPX can copy the encrypted IE into a cleartext IE in a request. Then the receiving SEPP decrypts the encrypted IE and puts its value into the cleartext IE field, resulting in the confidential IEs in N32-f message being exposed in the clear.
- *Threatened Asset*: SEPP Application, Service Messages to be sent/received over N32.

G.2.5 Threats related to TLS protection between NF and SEPP

G.2.5.1 Inter-PLMN routing using the incorrect reference

- *Threat name:* Inter-PLMN routing using the incorrect reference
- *Threat Category*: Denial of Service, Information Disclosure
- *Threat Description*: TLS protection between the SEPP and NFs within a PLMN may rely on using telescopic FQDN or 3gpp-Sbi-Target-apiRoot header. When telescopic FQDN is used between the NF and the SEPP, the NF shall use a telescopic FQDN in the Request URI of the HTTP Request to convey the target apiRoot to the SEPP. When 3gpp-Sbi-Target-apiRoot header is used between the NF and the SEPP, the NF shall use the 3gpp-Sbi-Target-apiRoot HTTP header in the HTTP Request to convey the target apiRoot to the SEPP. However, there may be the case that a potentially malicious or misbehaving NF would include both the 3gpp-Sbi-Target-apiRoot header and a request URI containing a telescopic FQDN when communicating with the SEPP. In this case, the SEPP is given two references for routing the NF request across PLMN. According to TS 33.501 [26] clause 13.1.1.1, when communication between the NF and the SEPP that generated the telescopic FQDN is based on using 3gpp-Sbi-Target-apiRoot header, the NF needs to use the telescopic FQDN in the 3gpp-Sbi-Target-apiRoot header of the HTTP Request. That means whenever the telescopic FQDN is available on the NF, it shall be used to convey the target apiRoot to the SEPP. If a malicious or misbehaving NF includes a 3gpp-Sbi-Target-apiRoot header containing an element different than the telescopic FQDN contained in the Request URI and the SEPP ignores the telescopic FQDN but uses the 3gpp-Sbi-Target-apiRoot header to route the request, the NF request will not be correctly routed. This can result in Denial of Service and Information Disclosure.
- *Threatened Asset*: SEPP Application, Service Messages to be sent/received over N32.

G.2.5.2 Tampering of Target API Root

- *Threat name:* Tampering of target API root
- *Threat Category*: Denial of Service, Information Disclosure
- *Threat Description*: TLS protection between the SEPP and NFs within a PLMN may rely on using telescopic FQDN or 3gpp-Sbi-Target-apiRoot header. Security mechanism negotiated between the SEPPs can be TLS security or PRINS security, and PRINS security shall be used if there are IPX entities on the path between the SEPPs. When PRINS security is used between the SEPPs and 3gpp-Sbi-Target-apiRoot header is used between the NF and the SEPP, the HTTP Request from the NF received by the SEPP will include the 3gpp-Sbi-Target-

apiRoot header, which is set to the apiRoot of the target NF. If the sending SEPP forwards the 3gpp-Sbi-Target-apiRoot header together with the HTTP Request on the N32-f interface, there are potentially two threats:

- Even if both negotiating SEPPs support the 3gpp-Sbi-Target-apiRoot custom HTTP header, the IPX entities on the path between the SEPPs may possibly not support this custom HTTP header, which will lead to failed message transmission. This can result in Denial of Service.
- Even if all the IPX entities on the path between the SEPPs support the 3gpp-Sbi-Target-apiRoot custom HTTP header, the apiRoot of the target NF in the 3gpp-Sbi-Target-apiRoot header could be potentially modified by a malicious IPX entity, which will lead to the message delivery to the incorrect target. This can result in Information Disclosure and Denial of Service.

- *Threatened Asset*: SEPP Application, Service Messages to be sent/received over N32.

Annex H: Aspects specific to the network product class NRF

H.1 Network product class description for the NRF

H.1.1 Introduction

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 this clause covers the aspects specific to the NRF network product class.

H.1.2 Minimum set of functions defining the NRF network product 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. Therefore, in order to define the NRF network product class, it is necessary to define the common set of 3GPP-defined functionalities that is constitutive for a NRF. As part of the NRF network product, it is expected that the NRF contains NRF application, a set of running processes (typically more than one) executing the software package for the NRF functions and OAM functions that are specific to the NRF network product model. Functionalities specific to the NRF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.518 [15].

Note: For the purposes of the present document, this common set is defined to be the list of functions contained in clause 6.2.6 of 3GPP TS 23.501 [8].

H.2 Assets and threats specific to the NRF

H.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the NRF to be protected are:

- NRF Application;
- NF profile of available NF instances: e.g. NF instance ID, NF type, PLMN ID, network slice related identifiers, FQND or IP address of NF, NF capacity information, NF priority information, Names of supported services, NF Specific Service authorization information, Location information for the NF instance, etc., as described in clause 6.2.6 of TS 23.501 [8].
- OAuth 2.0 Access Tokens for NF-NF authorization;
- The interfaces of NRF to be protected and which are within SECAM scope:
    - Service Based Interfaces to other NFs.
    - N27.
    - Console interface, for local access: local interface on NRF.
    - OAM interface, for remote access: interface between NRF and OAM system.

NOTE 1: The detailed interfaces of the NRF network product class are described in clause 4.3.6 of the present document.

- NRF Software: binary code or executable code

NOTE 2: NRF files could be any file owned by a user (root user as well as non root users), including user account data and credentials, log data, configuration data, OS files, NRF application, NF profile of available NF instances, OAuth 2.0 Access Tokens, or NRF Software.

H.2.2 Threats related to NRF authorization

H.2.2.1 No slice specific authorization for NF discovery

- *Threat name*: No slice specific authorization for NF discovery.
- *Threat Category*: Information Disclosure, Elevation of privilege.
- *Threat Description:* If NF discovery authorization for specific slice is not supported by the NRF, the NF instance in one slice can discover NF instances belonging to other slices. This can result in reduced assurance level of slice data isolation, making the system easily attacked as well as wasting resource.
- *Threatened asset:* NF profile of available NF instances.

Annex I:
Aspects specific to the network product class NEF

I.1 Network product class description for the NEF

I.1.1 Introduction

This annex captures the aspects specific to network product class NEF.

I.1.2 Minimum set of functions defining the NEF network product class

As part of the NEF network product, it is expected that the NEF to contain NEF application, a set of running processes (typically more than one) executing the software package for the NEF functions and OAM functions that are specific to the NEF network product model. Functionalities specific to the NEF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.519 [16].

Note: For the purposes of the present document, this common set is defined to be the list of NEF functions contained in clause 6.2.5 of 3GPP TS 23.501 [8].

I.2 Assets and threats specific to the NEF

I.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the NEF to be protected are:

- NEF Application;
- NF and User Data: e.g. NF capabilities and events, network and user sensitive information (e.g. DNN, S-NSSAI, etc.), structured data retrieved from UDR, 5G LAN group information, NWDAF analytics, etc.
- The interfaces of NEF to be protected and which are within SECAM scope:
  - Service based interface, Nnef, for providing services to SMF, and AF
  - Service based interface for consuming services from AMF, UDM, PCF, SMF, UDR, Binding Support Function, NRF
  - Console interface, for local access: local interface on NEF
  - OAM interface, for remote access: interface between NEF and OAM system

NOTE 1: The detailed interfaces of the NEF class are described in clause 4, Network Product Class Description of the present document.

- NEF Software: binary code or executable code

NOTE 2: NEF 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, NEF application, NF and User data, or NEF Software.

I.2.2 Threats related to NEF assets

I.2.2.1 No authentication on application function

- *Threat name:* No Authentication on application function
- *Threat Category:* Information Disclosure, tampering
- *Threat Description:* If the authentication of the Application Function is not supported, the application function without a legal certificates, or pre-shared key could be able to establish a TLS connection with the NEF. The data stored in the NEF may be exposed to an attacker.
- *Threatened Asset:* NF and User Data

I.2.2.2 No authorization on northbound APIs

- *Threat name:* No Authorization on northbound APIs
- *Threat Category:* Elevation of Privilege, Information Disclosure
- *Threat Description:* A malicious AF without OAuth-based authorization or with an incorrect access token may invoke the NEF services arbitrarily. For example, an attacker may invoke the Nnef_EventExposure_Subscribe service provide by the NEF without authorization. The Event data related with this subscribe will be leaked to the attacker.
- *Threatened Asset:* Sufficient Processing Capacity, NF and User Data

Annex J: Aspects specific to the network product class SMF

J.1 Network product class description for the SMF

J.1.1 Introduction

This Annex covers the aspects specific to the SMF network product class.

J.1.2 Minimum set of functions defining the SMF network product class

As part of the SMF network product, it is expected that the SMF to contain SMF application, a set of running processes (typically more than one) executing the software package for the SMF functions and OAM functions that is specific to the SMF network product model. Functionalities specific to the SMF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.511 [6].

Note: For the purposes of the present Annex, this common set is defined to be the list of SMF functions contained in 3GPP TS 23.501 [8].

J.2 Assets and threats specific to the SMF

J.2.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the SMF to be protected are:

- SMF Application;
- Session related data (e.g. subscriber's identities (e.g. SUPI), APN name, UE's IP address, QoS, etc.), network usage, charging data record, charging ID, etc.) ,
- User plane data,
- The interfaces of SMF to be protected and which are within SCAS scope:
    - Service based interface, Nsmf, for providing services to AMF, AF, NEF, and SMF
    - Service based interface for consuming services from UDM, AMF, PCF, NEF NRF, UDSF, CHF, and SMF
    - N4 interface
    - Console interface, for local access: local interface on SMF
    - OAM interface, for remote access: interface between SMF and OAM system

NOTE 1: The detailed interfaces of the SMF class are described in clause 4, Network Product Class Description of the present document.

- SMF Software: binary code or executable code

NOTE 2: SMF 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, SMF application, Mobility Management data or SMF Software.

J.2.2 Threats related to SMF assets

J.2.2.1 Priority of UP security policy

- *Threat name:* Non-compliant UP security policy handling

- *Threat Category:* Tampering data, Information Disclosure,

- *Threat Description:* It is required that user Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy in SMF. If SMF fails to comply with the requirement, user plane security may be degraded. For example, if the UP security policy from the UDM mandates the ciphering and integrity protection of the user plane data, but no protection is indicated in the local UP security policy at the SMF, and the local UP security policy takes the priority, then the user plane data will be sent over the air without any protection.

- *Threatened Asset:* User plane data

J.2.2.2 TEID uniqueness failure

- *Threat name:* Failure to assign unique TEID for a session

- *Threat Category:* Tampering data, Denial of Service, Information disclosure, Spoofing Identity

- *Threat Description:* TEID, as part of the CN Tunnel information, is used by the UPF and gNB/ng-eNB for user plane routing. The failure to guarantee the uniqueness of the TEID for a PDU session result in interruption of the routing of the user traffic. It also create charging errors. If multiple PDU sessions were to share the same TEID at the same time, the counts for the network usage of a single PDU session will be in fact the counts for the network usage of multiple sessions, creating charging errors.

- *Threatened Asset:* Session related data

J.2.2.3 Charging ID Uniqueness failure

- *Threat name:* Failure to assign unique Charging ID for a session.

- *Threat Category:* Tampering data, Information disclosure

- *Threat Description:* At the SMF if more than one PDU session were to share the same charging ID, the charging information for a PDU session would be wrongly correlated, creating charging errors.

- *Threatened Asset:* Session related data

J.2.2.3 UP security policy check

- *Threat name:* Unchecked UP security policy

- *Threat Category:* Tampering data, Information disclosure

- *Threat Description:* It is required that the SMF verifies that the UP security policy received from the ng-eNB/gNB is the same as that stored locally at the SMF. If the SMF fails to check, security degradation of UP traffic may occur. For example, if the UP security policy received from the ng-eNB/gNB indicates no security protection, while the local policy mandates the opposite, and SMF uses the received UP security policy without validation, then the user plane data will be unprotected.

- *Threatened Asset:* User plane data

Annex K: Aspects specific to the network product class AMF

K.1 Network product class description for the AMF

K.1.1 Introduction

This Annex covers the aspects specific to the AMF network product class.

K.1.2 Minimum set of functions defining the AMF network product class

As part of the AMF network product, it is expected that the AMF to contain AMF application, a set of running processes (typically more than one) executing the software package for the AMF functions and OAM functions that is specific to the AMF network product model. Functionalities specific to the AMF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.512 [22].

NOTE: For the purposes of the present document, this common set is defined to be the list of AMF functions contained in clause 6.2.5 of 3GPP TS 23.501 [8].

K.2 Assets and threats specific to the AMF

K.2.1 Critical assets

In addition to the critical assets of a GNP as described in clause 5.2 of the present document, the critical assets specific to the AMF to be protected are:

- AMF Application;
- Mobility Management data: e.g. subscriber's identities (e.g. SUCI), subscriber keys (I.e. K_{NASenc}, K_{NASint}, NH), authentication parameters, address of serving gNB, APN name, data related to mobility management like UE status, UE's IP address, etc., session management like PDN type, QoS and so on, or node selection and routing selection, e.g. IP address of UE related UPF, selected routing connection based on UE's identity, etc.
- The interfaces of AMF to be protected and which are within SECAM scope: for example
    - Service based interface, Namf, for providing services to SMF, AUSF, NEF, PCF, GMLC, SMSF, LMF and UDM
    - Service based interface for consuming services from NSSF, SMF, LMF, SMSF, PCF, 5G-EIR, UDM, AUSF, and NRF
    - Reference point interfaces:
        - N1.
        - N2.
        - N26.
    - Console interface, for local access: local interface on AMF.
    - OAM interface, for remote access: interface between AMF and OAM system.

NOTE 1: The detailed interfaces of the AMF class are described in clause 4, Network Product Class Description of the present document.

- AMF Software: binary code or executable code.

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

K.2.2 Threats related to AKA procedures

K.2.2.1 Resynchronization

- Threat name: Resynchronization
- Threat Category: Denial of Service
- Threat Description: If RAND and AUTS are not included when synchronization fails, the resynchronization procedure does not work correctly. This can result in waste of system resources and deny a legitimate user access to the system.
- Threatened Asset: Sufficient Processing Capacity

K.2.2.2 Failed Integrity check of Initial Registration message

- Threat name: Failed integrity check of Initial Registration message
- Threat Category: Denial of Service
- Threat Description: If integrity check of attach message fails, a user identity cannot be verified. This can result in waste of system resources and deny a legitimate user access to the system.
- Threatened Asset: Sufficient Processing Capacity

K.2.2.3 RES* verification failure

- Threat name: RES* verification failure
- Threat Category: Denial of Service
- Threat Description: If a malicious UE initiates a registration request using a SUCI and this request is followed by primary authentication in which an incorrect RES* is sent to the network, then the RES* verification will fail. In this case, if the RES* verification failure is not handled correctly, e.g., AMF/SEAF does not reject the registration request directly, or initiates a new authentication procedure with the UE, this would result in waste of system resources.
- Threatened Asset: Sufficient Processing Capacity

K.2.3 Threats related to security mode command procedure

K.2.3.1 Bidding Down

- Threat name: Bidding down
- Threat Category: Tampering of Data, Information Disclosure
- Threat Description: If SMC does not include the complete initial NAS message if either requested by the AMF or the UE sent the initial NAS message unprotected, the UE can force the system to reduce the security level by using weaker security algorithms or turning security off, making the system easily attacked and/or compromised.

- Threatened Asset: User account data and credentials

K.2.3.2 NAS integrity selection and use

- Threat name: NAS integrity selection and use
- Threat Category: Tampering of data, Information Disclosure, Denial of Service
- Threat Description: If NAS does not use the highest priority algorithm, NAS layer risks being exposed and/or modified or being exposed to denial of service.
- Threatened Asset: Sufficient Processing Capacity, Control plane signalling

K.2.3.3 NAS NULL integrity protection

- Threat name: NAS NULL integrity protection
- Threat Category: Elevation of Privilege
- Threat Description: If NAS NULL integrity protection is used outside of emergency call scenarios, an attacker can initiate unauthenticated non-emergency calls.
- Threatened Asset: Sufficient Processing Capacity

K.2.3.4 NAS confidentiality protection

- Threat name: NAS confidentiality protection
- Threat Category: Tampering of Data, Information Disclosure, Denial of Service
- Threat Description: If security mode complete message is not confidentiality protected, the AMF cannot be certain that the SMC is executed correctly. This can result in waste of system resources and deny a legitimate user access to the system.
- Threatened Asset: Sufficient Processing Capacity

K.2.4 Threats related to security in Intra-RAT mobility

K.2.4.1 Bidding down on Xn-Handover

- Threat name: Bidding down on Xn-Handover
- Threat Category: Tampering of Data, Information Disclosure
- Threat Description: If AMF cannot verify that the 5G security capabilities received from source gNB via the target gNB are the same as the UE security capabilities that the AMF has stored, the source gNB may force the system to accept a weaker security algorithm than the system is allowed forcing the system into a lowered security level making the system easily attacked and/or compromised.
- Threatened Asset: User account data and credentials

K.2.4.2 NAS integrity protection algorithm selection in AMF change

- Threat name: NAS integrity protection algorithm selection in AMF change
- Threat Category: Tampering of Data, Information Disclosure
- Threat Description: If the highest priority NAS integrity protection is not selected by the new AMF in AMF change, the new AMF could end up using a weaker algorithm forcing the system into a lowered security level making thee system easily attacked and/or compromised.

- Threatened Asset: User account data and credential

K.2.5 Threats related to release of non-emergency bearer

- Threat name: Release of non-emergency bearer
- Threat Category: Denial of Service
- Threat Description: If authentication fails in the AMF and the non-emergency bearer is not released, the UE can continue receiving unauthorized call, wasting valuable system resources.
- Threatened Asset: Sufficient Processing Capacity

K.2.6 Threats related to initial registration procedure

K.2.6.1 Invalid or unacceptable UE security capabilities

- Threat name: Invalid or unacceptable UE security capabilities
- Threat Category: Tampering of Data, Information Disclosure
- Threat Description: A flawed AMF implementation accepting insecure or invalid UE security capabilities may put User Plane and Control Plane traffic at risk, without the operator being aware of it. If NULL ciphering algorithm and/or NULL integrity protection algorithm of the UE security capabilities is accepted by the AMF, all the subsequent NAS, RRC, and UP messages will not be confidentiality and/or integrity protected. The attacker can easily intercept or tamper control plane data and the user plane data. This can result in information disclosure as well as tampering of data.
- Threatened Asset: User account data and credentials, Mobility Management data

K.2.7 Threats related to 5G-GUTI allocation

K.2.7.1 Failure to allocate new 5G-GUTI

- Threat name: Failure to allocate new 5G-GUTI.
- Threat Category: Information Disclosure.
- Threat Description: If a new 5G-GUTI is not allocated by AMF in certain registration scenarios (i.e. after receiving Registration Request message of type "initial registration", or Registration Request message of type "mobility registration update", or Service Request message sent by the UE in response to a Paging message), an attacker could keep on tracking the user using the old 5G-GUTI after these registration procedures. For a CIOT UE in idle state with suspend indication, even though the UE will not initiate Service Request after receiving a paging message, if a new 5G-GUTI is not allocated, the attacker can replay the paging message multiple times, and based on the responding messages the attacker could still be able to track the UE.
- Threatened Asset: Mobility Management data.

K.2.8 NAS based redirection from 5GS to EPS in 5G CIoT

- *Threat name:* NAS based redirection from 5GS to EPS
- *Threat Category*: Denial of Service, Information disclosure.
- *Threat Description*: In NAS based redirection from 5GS to EPS in 5G CIoT , when a UE initiates registration procedure with the AMF, the AMF may redirect the UE from 5GC to EPC with a Registration Reject message sent to the UE, and if the Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC is not protected, the attacker can modify the cause and the UE will try to connect to the EPS. This will lead to a bidding down attack to the UE.

- *Threatened Asset*: Sufficient Processing Capability, N1 interface, Mobility Management data.

K.2.9 Threat related to Security for 5G CIoT

K.2.9.1 Failed Verification of UE Identity during RRC Reestablishment Procedure for CP CIoT 5GS Optimization

- *Threat name:* failed Verification of UE Identity during RRC Reestablishment Procedure for CP CIoT 5GS Optimization
- *Threat Category*: Denial of Service.
- *Threat Description*: If veritification of UE using CP CIoT 5GS Optimization during RRC Reestablishment procedure fails, a user identity cannot be verified. This can result in waste of system resources and deny a legitimate user access to the system. In addition, if the AMF does not correctly indicate the ng-eNB result of veritication, an unlegal UE may successfully re-establish on the ng-eNB, and result in waste of system resources.
- *Threatened Asset*: Sufficient Processing Capacity.

K.2.10 Threats related to session establishment procedure

K.2.10.1 Incorrect validation of S-NSSAIs

- *Threat name*: Incorrect Validation of S-NSSAIs.
- *Threat category*: Elevation of Privilege.
- *Threat Description*: After the successful network slice-specific authentication and authorization, there will be an Allowed NSSAI list both in UE and AMF. Then, the UE will initiate the PDU session establishment request with the requested S-NSSAIs included. If the AMF does not verify whether the received S-NSSAIs is within the Allowed NSSAI list stored at the AMF, an attacker can still include the rejected S-NSSAIs in the request and access the slice after it fails the NSSAA procedure.
- *Threatened Asset:* Mobility management data, sufficient processing capacity.

Annex L: Aspects specific to the network product class UPF

L.1 Network product class description for the UPF

L.1.1 Introduction

This Annex covers the aspects specific to the UPF network product class.

NOTE: Operators can deploy UPF(s) supporting the Inter PLMN User Plane Security (IPUPS) functionality at the border of their network as specified in TS 23.501[26] clause 5.8.2.14.

L.1.2 Minimum set of functions defining the UPF network product class

As part of the UPF network product, it is expected that the UPF contains UPF application, a set of running processes (typically more than one) executing the software package for the UPF functions and OAM functions that are specific to the UPF network product model. Functionalities specific to the UPF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.513 [18].

Note: For the purposes of the present Annex, this common set is defined to be the list of functions contained in clause 6.2.3 in 3GPP TS 23.501 [8].

L.2 Assets and threats specific to the UPF

L.2.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the UPF to be protected are:

- UPF Application;
- User plane data;
- Session related data, e.g. CN Tunnel information, packet detection rules, network usage, traffic detection information, and etc.;
- Security data, i.e. cryptographic materials for N3, N4 and N9 interfaces
- The interfaces of the UPF to be protected and which are within SECAM scope:
  - N3 interface between the UPF and the gNB/ng-eNB
  - N4 interface between the UPF and the SMF
  - N6 interface between the UPF and the DN
  - N9 interface between two UPFs
  - Console interface, for local access: local interface on the UPF
  - OAM interface, for remote access: interface between the UPF and the OAM system

NOTE 1: The detailed interfaces of the UPF class are described in clause 4 of the present document.

- UPF Software: binary code or executable code

NOTE 2: UPF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, UPF application, user plane security mechanism, or cryptographic materials.

L.2.2 Threats related to user plane data transport

- *Threat name:* No protection or weak protection for user plane data.

- *Threat Category:* Tampering, Information Disclosure.

- *Threat Description:* User traffic is transported between the gNB/ng-eNB and the UPF via N3 interface, or between two UPFs within a PLMN via N9 interface. If the user traffic transported over the interfaces is not confidentiality protected, it can be subject to eavesdropping. Information is leaked to unauthorized parties. If the user traffic is not integrity protected, attackers can tamper with user traffic at will. The receiver of the user traffic obtain false user traffic. If the user traffic is not replay protected, attackers can insert historical legitimate user traffic. This can lead to false network usage reported by the UPF, and consequently resulting in billing fraudulence.

  If the protection implemented for the user plane data transported over the N3 interface and the N9 interface within a PLMN uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the user plane data may be degraded and fail to fulfil the required security.

- *Threatened Asset:* User plane data.

L.2.3 Threats related to signalling data

- *Threat name:* No protection or weak protection for signalling data over N4 interface

- *Threat Category:* Denial of service, tampering.

- *Threat Description:* SMF controls the user plane path of PDU sessions through N4 interfaces. If the signalling data over N4 interface is not protected e.g. against tampering, the user traffic may be wrongly routed and fail to arrive at the intended recipient. This can create Denial of Service.

  To support billing, UPF reports network usage to SMF over N4 interface. Unprotected network usage report can lead to billing fraud.

  If the protection implemented for the signalling data over the N4 interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the security level of the signalling data transported over N4 interface may be degraded and fail to fulfil the required security.

- *Threatened Asset:* session related data.

L.2.4 Threats related to TEID

- *Threat name:* Failure to assign unique TEID for a session.

- *Threat Category:* Tampering.

- *Threat Description:* TEID, as part of the CN Tunnel information, is used by the UPF and gNB/ng-eNB for user plane routing. The failure to guarantee the uniqueness of the TEID for a PDU session interrupts the routing of user traffic. It also interrupts charging. If multiple PDU sessions were to share the same TEID at the same time, the counts for the network usage of a single PDU session will be in fact the counts for the network usage of multiple sessions, creating charging errors.

- *Threatened Asset:* session related data.

L.2.5 Threats related to user plane data forwarding

- *Threat name:* invalid user plane data forwarding.

- *Threat Category:* Tampering, Information Disclosure, Denial of Service.

- *Threat Description:* User plane traffic is transported between UPFs over the N9 interface. If the UPF with IPUPS functionality fails to discard GTP-U packets that do not belong to any active PDU sessions, routing of user plane traffic could be interrupted or Denial of Service attacks to the network could be possible.This threat only applies if the UPF implements the IPUPS functionality.

- *Threatened Asset*: User plane data.

L.2.6 Threats related to malformed GTP-U messages

- Threat name: Threats of malformed GTP-U messages.

- Threat Category: Denial of service.

- Threat Description: Malicious sender may send malformed GTP-U messages to a victim UPF with IPUPS functionality. If the malformed GTP-U messages are not filtered, they may consume the processing resource of the victim UPF with IPUPS functionality, and even cause the victim UPF functionality to crash, causing denial of service attack.

- Threatened Asset: Sufficient Processing Capacity.

Annex M:
Aspects specific to the network product class N3IWF

M.1 Threat to send EAP-Identity Request by N3IWF

- *Threat name:* N3IWF sends EAP-Identity Request
- *Threat Category*: Denial of service.
- *Threat Description*: EAP-5G is used between UE and N3IWF. As specificed in TS 33.501[14], the N3IWF shall refrain from sending an EAP-Identity request. The UE may ignore an EAP Identity request or respond with the SUCI it sent in the Registration Request. This means if the N3IWF happens to send an EAP-Identity Request to the UE, the N3IWF shall not look forward an EAP-Identity Reply. This is different from normal EAP framework. If the N3IWF behaves the same as normal EAP framework, the N3IWF will wait for a reply till time expires. This may casue the UE cannot access to the network via an N3IWF.
- *Threatened Asset*: GNP services.

Annex N:
Aspects specific to the network product class NWDAF

N.1 Network product class description for the NWDAF

N.1.1 Introduction

This Annex covers the aspects specific to the NWDAF network product class.

N.1.2 Minimum set of functions defining the NWDAF network product class

As part of the NWDAF network product, it is expected that the NWDAF to contain NWDAF application (for data analysis), a set of running processes (typically more than one) executing the software package for the NWDAF functions and OAM functions that is specific to the NWDAF network product model. Functionalities specific to the NWDAF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.521 [23].

NOTE: For the purposes of the present document, this common set is defined to be the list of NWDAF functions contained in clause 6.2.18 of 3GPP TS 23.501 [8].

N.2 Assets and threats specific to the NWDAF

N.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the NWDAF to be protected are:

- NWDAF Application;
- Collected Data from NFs: e.g. part of mobility management data as depicted in clause K.2.1 collected from AMF, part of Session related data, user plane data as depicted in clause J.2.1 collected from SMF, part of user subscription data as depicted in clause E.2.1 collected from UDM, part of NF and User Data as depicted in clause I.2.1 collected from NEF, data collectd from NRF, PCF, AF and OAM, etc.
- The interfaces of NWDAF to be protected and which are within SECAM scope:
  - Service based interface, Nnwdaf, for providing services to AMF, SMF, NEF, PCF, NSSF, OAM and AF.
  - Service based interface for consuming services from AMF, SMF, UDM, PCF, NRF, NEF and AF.
    - Console interface, for local access: local interface on NWDAF
    - OAM interface, for remote access and data collection: interface between NWDAF and OAM system

NOTE 1: The detailed interfaces of the NWDAF class are described in clause 4, Network Product Class Description of the present document.

- NWDAF Software: binary code or executable code

NOTE 2: NWDAF 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, NWDAF application, Collected Data from NFs or NWDAF Software.

N.2.2 Void

Annex O: Aspects specific to the IMS network product classes

O.1 Network product class description for the IMS

O.1.1 Introduction

This Annex covers the aspects specific to the IMS network products with specific threats.

O.1.2 Minimum set of functions defining the IMS network product classes

As part of the IMS network products, it is expected that the IMS network product classes (e.g. P-CSCF) contains IMS network product classes application, a set of running processes (typically more than one) executing the software package for the IMS network product functions and OAM functions that are specific to the IMS network product model. Functionalities specific to the IMS network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.226 [25].

Note: For the purposes of the present Annex, this common set is defined to be the list of functions contained in clause 4.0 in 3GPP TS 23.228 [24].

O.2 Assets and threats specific to the P-CSCF

O.2.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the P-CSCF to be protected are:

- P-CSCF Application;
- IMS signalling;
- Security data, i.e. cryptographic materials for Gm, Mw, Mx, and Iq interfaces
- The interfaces of the P-CSCF to be protected and which are within SECAM scope:
    - Gm interface between the P-CSCF and UE
    - Mw interface between the P-CSCF and the C-CSCF/I-CSCF
    - Mx interface between the P-CSCF and IBCF
    - Iq interface between the P-CSCF and IMS AGW
    - Console interface, for local access: local interface on the P-CSCF
    - OAM interface, for remote access: interface between the P-CSCF and the OAM system

NOTE 1: The detailed interfaces of the P-CSCF class are described in clause 4 of the present document.

- P-CSCF Software: binary code or executable code

NOTE 2: P-CSCF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, P-CSCF application, user plane security mechanism, or cryptographic materials.

O.2.2 Threats related to set-up of security associations

O.2.2.1 High-priority algorithm selection

- Threat name: High-priority algorithm selection
- Threat Category: Tampering of data, Information Disclosure, Denial of Service
- Threat Description: If the P-CSCF does not select the highest priority algorithm combination on its own list which is also supported by the UE to protect the messages between the P-CSCF and the UE, the P-CSCF could end up using a weaker algorithm forcing the system into a lowered security level making the system easily attacked and/or compromised.
- Threatened Asset: IMS signalling

O.2.2.2 Bidding down on security association set-up

- Threat name: Bidding down on security association set-up
- Threat Category: Tampering of data, Information Disclosure, Denial of Service
- Threat Description: If the P-CSCF does not check whether the integrity and encryption algorithms list, SPI_P and Port_P received in SM7 is identical with the corresponding parameters sent in SM6, and check whether SPI_U and Port_U received in SM7 are identical with those received in SM1, the attacker can force the system to reduce the security level by tampering the integrity and encryption algorithms list. Then, weaker security algorithms may be selected, which will make the system easily attacked. Tampering the SPI will cause the negotiated SA cannot be indexed. As a result, the following security association fails to be established, leading to Denial of Service attack. The port number is generally used to identify different applications. Tampering the Port_P number by the attacker will cause messages to be sent to the UE or P-CSCF through the tampered port. These messages including some sensitive parameters may be leaked to another application, which is not intended to receive this message.
- Threatened Asset: IMS signalling, security data

O.2.3 Threats related to IMS signalling transport

- *Threat name:* No protection or weak protection for IMS signalling data.
- *Threat Category:* Tampering, Information Disclosure.
- *Threat Description:* The following behaviours may lead to bidding down attacks
    - If the protection implemented for the IMS signalling over Gm interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the IMS signalling data may be degraded and fail to fulfil the required security.
    - If the P-CSCF policy requires confidentiality, then all UEs with no encryption support would be denied access to the IMS network. For example, if the UE sends the NULL encryption algorithm to the P-CSCF in SM1, and the SM1 message is not denied by the P-CSCF, the following negotiated SA between UE and P-CSCF may be established without confidentiality protection, which disobeys the P-CSCF policy requiring confidentiality. Hence, the following IMS signalling data will be leaked.

- *Threatened Asset:* IMS signalling data.

O.2.4 Threats related to SPI allocation

- *Threat name:* Same SPIs between UE and P-CSCF.
- *Threat Category:* Information disclosure, Denial of service.

- *Threat Description:* If the P-CSCF selects the same SPIs as received in the *Security-setup-line* from the UE, the attacker could reflect the old messages back to P-CSCF. Since the UE and the P-CSCF use the same key for inbound and outbound traffic, the P-CSCF will decrypt the reflected messages correctly with the same key, and perform the following operation accordingly. Hence, the P-CSCF will suffer reflection attacks. The information may leak within the response message as required by the reflected message, or the ongoing services may be interrupted. The attack is also applicable on the UE side.

- *Threatened Asset:* IMS signalling, P-CSCF application.

O.3 Assets and threats specific to the S-CSCF

O.3.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the S-CSCF to be protected are:

- S-CSCF Application;
- IMS signalling;
- Security data, i.e. cryptographic materials for Mw, Mx, Mm, Mg, ISC, Cx, Dx, Mr, and Mi interfaces
- The interfaces of the S-CSCF to be protected and which are within SECAM scope:
    - Mw interface between the S-CSCF and I-CSCF/P-CSCF
    - Mx interface between the S-CSCF and IBCF
    - Mm interface between the S-CSCF and IP multimedia network
    - Mg interface between the S-CSCF and MGCF
    - ISC interface between the S-CSCF and AS
    - Cx interface between the S-CSCF and HSS
    - Dx interface between the S-CSCF and SLF
    - Mr interface between the S-CSCF and MRFC
    - Mi interface between the S-CSCF and BGCF
    - Console interface, for local access: local interface on the P-CSCF
    - OAM interface, for remote access: interface between the P-CSCF and the OAM system

NOTE 1: The detailed interfaces of the S-CSCF class are described in clause 4 of the present document.

- S-CSCF Software: binary code or executable code

NOTE 2: S-CSCF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, S-CSCF application, user plane security mechanism, or cryptographic materials.

O.3.2 Threats related to de-registration during the authentication

- *Threat name:* No de-registration during the authentication.

- *Threat Category:* Denial-of-service attack.

- *Threat Description:* Assume that a legal UE has already been registered into the IMS network with the IMPU. An attacker could try to register an already registered IMPU and respond with an incorrect authentication response in order to make the HN de-register the IMPU of the legal UE. In this case, the legal UE will be de-registered in the HSS. Therefore, the attacker could open up a potential denial-of-service attack deny a legitimate user access to the system.

- *Threatened Asset:* Sufficient Processing Capacity.

O.3.3 Threats related to authenticated re-registration

O.3.3.1 Unprotected register message

- Threat name: Unprotected REGISTER messages
- Threat Category: Tampering of data, Information Disclosure, Denial of Service
- Threat Description: If the S-CSCF does not authenticate the user by means of the AKA protocol in case of the UE sends unprotected REGISTER messages, the attacker without a legal certificates, or pre-shared key could be able to access the network. The data and resources stored in the network may be exposed to an attacker, making the system easily attacked and/or compromised.
- Threatened Asset: S-CSCF Application, Security data

O.3.3.2 No resynchronization

- *Threat name:* No resynchronization
- *Threat Reference*: Denial of Service
- *Threat Description*: In the synchronization failure scenario, after receiving the CM4 message from HSS, the UE may not be able to access to the network if no new authentication procedure is triggered by the S-CSCF, i.e. the UE is given no opportunity to resynchronize with the network. This can result in waste of system resources and deny a legitimate user access to the system.
- *Threatened Asset*: Sufficient Processing Capacity

O.4 Assets and threats specific to the I-CSCF

O.4.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the I-CSCF to be protected are:

- I-CSCF Application
- IMS signalling, the Address of the S-CSCF, Charging data records
- Security data, i.e. cryptographic materials for Mw, Cx, Mx, Ma, and Mm interfaces
- The interfaces of the I-CSCF to be protected and which are within SECAM scope:
    - Mw interface between the I-CSCF and S-CSCF/P-CSCF
    - Cx interface between the I-CSCF and the HSS and SLF
    - Mx interface between the I-CSCF and the IBCF
    - Ma interface between the I-CSCF and AS
    - Mm interface between the I-CSCF and IP Multimedia Networks
    - Console interface, for local access: local interface on the I-CSCF

  - OAM interface, for remote access: interface between the I-CSCF and the OAM system

NOTE 1: The detailed interfaces of the I-CSCF class are described in clause 4 of the present document.

- I-CSCF Software: binary code or executable code

NOTE 2: I-CSCF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, I-CSCF application, user plane security mechanism, or cryptographic materials.

O.4.2 Threats related to network hiding

O.4.2.1 encryption in network hiding

- Threat name: Encryption in network hiding
- Threat Category: Spoofing identity, Tampering of data, Information Disclosure
- Threat Description: In casse of the network hiding mechanism is used and the operator policy states that the topology shall be hidden, if the encryption of the hiding information elements is not performed when the I-CSCF forwards SIP Request or Response messages outside the hiding network's domain, and the decryption of the hiding information elements is not performed when the I-CSCF receives a SIP Request or Response message from the outside of the hiding network's domain, the identities of the SIP proxies and the topology of the hiding network will not be protected, and an attacker can read or modify these information elements.

- Threatened Asset: IMS signalling

O.5 Assets and threats specific to the IBCF

O.5.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the IBCF to be protected are:

- IBCF Application
- IMS signalling, Network configuration hiding, Charging data records
- Security data, i.e. cryptographic materials for Mx, Cs, Ix, and Ici interfaces
- The interfaces of the IBCF to be protected and which are within SECAM scope:
  - Mx interface between the IBCF and S-CSCF/P-CSCF/I-CSCF/BGCF
  - Ms interface between the IBCF and the AS
  - Ix interface between the IBCF and the TrGW
  - Ici interface between the IBCF and IP Multimedia Networks
  - Console interface, for local access: local interface on the IBCF
  - OAM interface, for remote access: interface between the IBCF and the OAM system

NOTE 1: The detailed interfaces of the IBCF class are described in clause 4 of the present document.

- IBCF Software: binary code or executable code

NOTE 2: IBCF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, IBCF application, user plane security mechanism, or cryptographic materials.

O.5.2 Threats related to network hiding

O.5.2.1 encryption in network hiding

- Threat name: Encryption in network hiding
- Threat Category: Spoofing identity, Tampering of data, Information Disclosure
- Threat Description: In cases of the encryption of the hiding information as network hiding mechanism is used and the operator policy states that the topology shall be hidden, and the encryption of the hiding information elements is not performed when the IBCF forwards SIP Request or Response messages outside the hiding network's domain, and the decryption of the hiding information elements is not performed when the IBCF receives a SIP Request or Response message from the outside of the hiding network's domain, the identities of the SIP proxies and the topology of the hiding network will not be protected, and an attacker can read or modify these information elements.
- Threatened Asset: IMS signalling

O.5.2.2 replacement in network hiding

- Threat name: Replacement in network hiding
- Threat Category: Spoofing identity, Tampering of data, Information Disclosure
- Threat Description: In cases of the replacement of the hiding information as network hiding mechanism is used and the operator policy states that the topology shall be hidden, and the hiding information elements are not replaced to constant values when the IBCF forwards SIP Request or Response messages outside the hiding network's domain, and the constant values are not replaced to the hiding information elements when the IBCF receives a SIP Request or Response message from the outside of the hiding network's domain, the identities of the SIP proxies and the topology of the hiding network will not be protected, and an attacker can read or modify these information elements.

- Threatened Asset: IMS signalling

O.6 Assets and threats specific to the AS

O.6.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the AS deployed in the user's home network to be protected are:

- AS Application
- IM service data
- Security data, i.e. cryptographic materials for Ma, Ms, ISC, Rc, Cr, Sh, and Dh interfaces
- The interfaces of the IBCF to be protected and which are within SECAM scope:
    - Ma interface between the AS and I-CSCF
    - Ms interface between the AS and the IBCF
    - ISC interface between the AS and S-CSCF
    - Rc interface between the AS and MRB

- Cr interface between the AS and MRFC
- Sh interface between the AS and HSS
- Dh interface between the AS and SLF
- Console interface, for local access: local interface on the AS
- OAM interface, for remote access: interface between the AS and the OAM system

NOTE 1: The detailed interfaces of the AS class are described in clause 4 of the present document.

- AS Software: binary code or executable code

NOTE 2: AS files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, AS application, user plane security mechanism, or cryptographic materials.

O.6.2 Threats related to authorization

O.6.2.1 No user authorization

- Threat name: No user identity authorization
- Threat Category: Elevation of privilege
- Threat Description: It was described that once the AS have tried to verify the identity of the user, the AS either has a verified identity of the user or it considers the user as anonymous. If the AS configured that anonymous user is not allowed, does not reject the anonymous service request, the attacker could request functioanlity using the anonymous idenity without any authorizaiton.
- Threatened Asset: IMS signalling, security data

O.6.2.1 No ID privacy

- Threat name: No ID privacy
- Threat Category: Information Disclosure
- Threat Description: It was described where privacy is required, in any initial request for a dialog or request for a standalone transaction, the AS shall set a display-name of the From header field to "Anonymous"and set an addr-spec of the From header field to Anonymous User Identity. If the AS does not set the ID to anonymous, the content of the From header field will be leaked.

- Threatened Asset: IMS signalling, security data

O.7 Assets and threats specific to the MRFC

O.7.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the MRFC to be protected are:

- MRFC Application
- Media stream resource, Charging data records
- Security data, i.e. cryptographic materials for Mp, Mr, and Cr/Mr' interfaces

- The interfaces of the MRFC to be protected and which are within SECAM scope:
    - Mp interface between the MRFC and MRFP
    - Mr interface between the MRFC and the S-CSCF
    - Cr/Mr' interface between the MRFC and AS
    - Console interface, for local access: local interface on the MRFC
    - OAM interface, for remote access: interface between the MRFC and the OAM system

NOTE 1: The detailed interfaces of the MRFC class are described in clause 4 of the present document.

- MRFC Software: binary code or executable code

NOTE 2: MRFC files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, MRFC application, user plane security mechanism, or cryptographic materials.

O.8 Assets and threats specific to the IMS AGW

O.8.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the IMS AGW to be protected are:

- IMS AGW Application;
- Media stream resource;
- Security data, i.e. cryptographic materials for Iq and Mp interfaces
- The interfaces of the IMS AGW to be protected and which are within SECAM scope:
    - Iq interface between the IMS AGW and P-CSCF
    - Mb interface between the IMS AGW and IMS MGW
    - Console interface, for local access: local interface on the IMS AGW
    - OAM interface, for remote access: interface between the IMS AGW and the OAM system

NOTE 1: The detailed interfaces of the IMS AGW class are described in clause 4 of the present document.

- IMS AGW Software: binary code or executable code

NOTE 2: IMS AGW files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, IMS AGW application, user plane security mechanism, or cryptographic materials.

O.9 Assets and threats specific to the MRFP

O.9.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the MRFP to be protected are:

- MRFP Application

- Media stream resource
- Security data, i.e. cryptographic materials for Mp interface
- The interfaces of the MRFP to be protected and which are within SECAM scope:
  - Mp interface between the MRFC and MRFP
  - Console interface, for local access: local interface on the MRFP
  - OAM interface, for remote access: interface between the MRFP and the OAM system

NOTE 1: The detailed interfaces of the MRFP class are described in clause 4 of the present document.

- MRFP Software: binary code or executable code

NOTE 2: MRFP files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, MRFP application, user plane security mechanism, or cryptographic materials.

O.10 Assets and threats specific to the IMS MGW

O.10.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the IMS MGW to be protected are:

- IMS MGW Application;
- Media stream resource;
- Security data, i.e. cryptographic materials for Mn, Mb, and CS interfaces
- The interfaces of the IMS MGW to be protected and which are within SECAM scope:
  - Mn interface between the IMS MGW and MGCF
  - Mb interface between the IMS MGW and MRFP/IMS AGW
  - CS interface between the IMS MGW and CS Network
  - Console interface, for local access: local interface on the IMS AGW
  - OAM interface, for remote access: interface between the IMS MGW and the OAM system

NOTE 1: The detailed interfaces of the IMS MGW class are described in clause 4 of the present document.

- IMS MGW Software: binary code or executable code

NOTE 2: IMS MGW files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, IMS MGW application, user plane security mechanism, or cryptographic materials.

O.11 Assets and threats specific to the TrGW

O.11.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the TrGW to be protected are:

- TrGW Application;
- Media stream resource;
- Security data, i.e. cryptographic materials for Ix and Izi interfaces
- The interfaces of the TrGW to be protected and which are within SECAM scope:
    - Ix interface between the TrGW and IBCF
    - Izi interface between the TrGW and IP Multimedia Network
    - Console interface, for local access: local interface on the TrGW
    - OAM interface, for remote access: interface between the TrGW and the OAM system

NOTE 1: The detailed interfaces of the TrGW class are described in clause 4 of the present document.

- TrGW Software: binary code or executable code

NOTE 2: TrGW files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, TrGW application, user plane security mechanism, or cryptographic materials.

O.12 Assets and threats specific to the MGCF

O.12.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the IMS AGW to be protected are:

- MGCF Application;
- Media stream resource;
- Security data, i.e. cryptographic materials for Mg, Mj, CS, and Mn interfaces
- The interfaces of the MGCF to be protected and which are within SECAM scope:
    - Mg interface between the MGCF and I-CSCF
    - Mj interface between the MGCF and BGCF
    - CS interface between the MGCF and CS Network
    - Mn interface between the MGCF and IM MGW
    - Console interface, for local access: local interface on the IMS AGW
    - OAM interface, for remote access: interface between the IMS AGW and the OAM system

NOTE 1: The detailed interfaces of the IMS AGW class are described in clause 4 of the present document.

- IMS AGW Software: binary code or executable code

NOTE 2: IMS AGW files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, IMS AGW application, user plane security mechanism, or cryptographic materials.

Annex P: Aspects specific to the network product class NSSAAF

P.1 Void

P.2 Network product class description for the NSSAAF

P.2.1 Introduction

This annex captures the aspects specific to network product class NSSAAF.

P.2.2 Minimum set of functions defining the NSSAAF network product class

As part of the NSSAAF network product, it is expected that the NSSAAF to contain NSSAAF application, a set of running processes (typically more than one) executing the software package for the NSSAAF functions and OAM functions that is specific to the NSSAAF network product model. Functionalities specific to the NSSAAF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.326 [29].

NOTE: For the purposes of the present document, this common set is defined to be the list of NSSAAF functions contained in clause 6.2.23 of 3GPP TS 23.501 [8].

P.3 Assets and threats specific to the NSSAAF

P.3.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the NSSAAF to be protected are:

- NSSAAF Application;
- User Data: e.g. subscriber's identities (e.g. GPSI), S-NSSAIs, EAP authentication parameters (e.g. EAP ID), etc.
- Slice information: e.g. the the (S-NSSAI, ENSI) mappings
- The interfaces of NSSAAF to be protected and which are within SECAM scope:
    - Service based interface, N_{NSSAAF}, for providing services to AMF
    - Service based interface for consuming services from UDM, and AMF
    - Console interface, for local access: local interface on NSSAAF
    - OAM interface, for remote access: interface between NSSAAF and OAM system
    - AAA interface: interface betweeen NSSAAF and AAA-P or AAA-S

NOTE 1: The detailed interfaces of the NSSAAF class are described in clause 4, Network Product Class Description of the present document.

- NSSAAF Software: binary code or executable code

NOTE 2: NSSAAF 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, NSSAAF application, user data or NSSAAF Software.

NOTE 3: The slice information is only applicable when AAA-S belongs to the 3rd party and the mapping of S-NSSAI to ENSI is needed.

P.3.2 Threats related to NSSAAF

P.3.2.1 Threats related to impersonating attack by AAA-S

- *Threat name:* Threats related to impersonating attack by AAA-S
- *Threat Category*: Denial of service, spoofing identity
- *Threat Description*: Network slice specific authentication and authorization (NSSAA) is performed between UE and AAA server (AAA-S). AAA-S may also trigger network slice-specific authorization revocation by sending a request to NSSAAF. After receiving the request to revoke the slice-specific authorization for a slice for a UE from an AAA-S, if NSSAAF does not check whether the AAA-S is legitimate in the sense that it had performed the NSSAA for the slice for the UE, a malicious AAA-S may masquerade as the legitimate AAA-S to invoke the slice-specific authorization for the slice for the UE. Then UE is denied access to the slice. Similarly a malicious AAA-S may also trick NSSAAF to perform slice specific re-authentication and re-authorization just to incur extra signalling load.
- *Threatened Asset*: user data related to NSSAA, processing capacity

P.3.2.2 Threat to select AAA-P and AAA-S

- *Threat name:* AAA-P and AAA-S wrong selection
- *Threat Category*: Denial of service.
- *Threat Description*: AAA-S in NSSAA procedure may be hosted by the HPLMN or third party which has a business relationship. When AAA-S belongs to a third party, the AAA-P in the HPLMN may be involved. Different S-NSSAI may go to different AAA-S. If the NSSAAF does not have the ability to select the right receiver, the authentication will always fail.
- *Threatened Asset*: GNP Application.

Annex Q (normative): Aspects specific to the network product class SCP

Q.1 Network product class description for the SCP

Q.1.1 Introduction

This Annex covers the aspects specific to the SCP network product class.

Q.1.2 Minimum set of functions defining the SCP network product 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. Therefore, in order to define the SCP network product class, it is necessary to define the common set of 3GPP-defined functionalities that is constitutive for a SCP. As part of the SCP network product, it is expected that the SCP contains SCP application, a set of running processes (typically more than one) executing the software package for the SCP functions and OAM functions that is specific to the SCP network product model. Functionalities specific to the SCP network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.522 [27].

Note: For the purposes of the present document, this common set is defined to be the list of functions contained in clause 6.2.19 of 3GPP TS 23.501 [28].

Q.2 Assets and Threats specific to SCP

Q.2.1 Threats related to tokens handled by the SCP

Q.2.1.1 Token forwarded to a wrong pNF instance

- *Threat name:* Token forwarded to a wrong pNF instance
- *Threat Category*: Denial of Service, Information Disclosure, Spoofing Identity, Elevation of Privilege
- *Threat Description*: According to TS 33.501 [14] clauses 13.4.1.3, the SCP is able to obtain the access token and/or client credentials assertion from the consumer NF, which are/is forwarded to the producer NF for authorization and/or authentication. If the SCP failed to select the correct target pNF instance due to e.g. mis-implementation or misconfiguration or weak internal interface protection, which results in the token being forwarded to the wrong pNF instance, there are the following threats:
    - The pNF instance receiving the access token will not be able to verify the access token, hence leading to authorization failure for indirect communication. Consequently, the access token, as a piece of sensitive information of the cNF, is exposed to a NF instance which is not meant to have it. This can result in denial of service, information disclosure, as well as waste of system resources. In worse case, if the NF instance receiving the access token wants to access the service granted in the token but not granted to the NF, it may impersonate the cNF to invoke the service of the target pNF using the received access token. This can result in spoofed identity and elevation of privilege.
    - The pNF instance receiving the client credentials assertion will not be able to verify the assertion, hence leading to failure of authenticating the cNF. Consequently, the credentials assertion, as a piece of sensitive information of the cNF, is exposed to a NF instance which is not meant to have it. This can result in denial of service, information disclosure, as well as waste of system resources. In worse case, if the NF instance receiving the assertion wants to access the service granted in the token but not granted to the NF, it may impersonate the cNF using the assertion for authentication with the target pNF, so as to facilitate the service

access to the target pNF with the exposed access token. This can result in spoofed identity and elevation of privilege.

- *Threatened Asset*: SCP Application, Access Tokens, Client Credentials Assertions, Service Messages forwarded/routed between NFs/NF services, Sufficient Processing Capacity

Q.2.1.2 Swapped token forwarded to the target pNF

- *Threat name:* Swapped token forwarded to the target pNF
- *Threat Category*: Denial of Service, Information Disclosure, Spoofing Identity, Elevation of Privilege
- *Threat Description*: When NFs and NF services communicate indirectly via the SCP, the SCP may receive multiple access tokens, which could come from multiple cNFs requesting services or from a single cNF requesting access to various services or network slices provided by the target pNFs. Particularly for indirect communication with delegated discovery, the SCP is delegated to request access tokens from the NRF for service requests from cNFs and then include the correct access token in each of the service requests from cNFs. If the SCP mixes-up the received multiple access tokens and includes the wrong access token in a service request, due to mis-implementation or misconfiguration, there are the following threats:
    - During indirect communication with delegated discovery, if the SCP mistakenly includes an access token of the requesting cNF destined for a pNF different from the target pNF (i.e. audience mismatch), the target pNF will fail to verify the access token, hence leading to authorization failure for indirect communication. Consequently, the access token, as a piece of sensitive information of the cNF, is exposed to a NF instance which is not meant to have it. This can result in denial of service as well as waste of system resources. In worse case, if the target NF wants to access the service granted in the token but not granted to the NF, it may impersonate the cNF to invoke the service of another pNF using the received access token. This can result in spoofed identity and elevation of privilege.
    - During indirect communication with delegated discovery, if the SCP mistakenly includes the access token of a cNF different from the requesting cNF (i.e. subject mismatch) or includes an access token of the requesting cNF for a service/slice different from the requested service/slice (i.e. scope mismatch), the target pNF will fail to verify the access token, hence leading to authorization failure for indirect communication. This can result in denial of service as well as waste of system resources.
    - During indirect communication with delegated discovery, if the SCP includes the correct access token but mistakenly includes a client credentials assertion of another cNF, the target pNF will fail to verify the assertion, hence leading to authentication failure for indirect communication. This can result in denial of service as well as waste of system resources.
- *Threatened Asset*: SCP Application, Service Messages forwarded/routed between NFs/NF services, Sufficient Processing Capacity

Annex R: Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2016-06	SA#72					Upgrade to version under change control	13.0.0
2016-09	SA#73	SP-160577	0001	1	F	Remove “shall” from the TR	13.1.0
2017-03	SA#75					Promotion to Release 14 without technical change	14.0.0
2017-06	SA#76	SP-170512	0002	1	B	Adding a generic threat on “User Session Tampering”	15.0.0
2017-09	SA#77	SP-170641	0003	-	B	Adding PWG Annex to TR33.926	15.1.0
2017-09	SA#77	SP-170641	0004	-	B	Adding eNB Annex to Support SCAS_eNB	15.1.0
2019-06	SA#84	SP-190361	0006	1	B	Addition of AMF-related Security Problem Descriptions: Not implemented as it was intended as draft CR (MCC).	16.0.0
2019-06	SA#84	SP-190361	0007	1	B	Adding gNB Annex	16.0.0
2019-06	SA#84					Removal of annex X.2 added by accident (MCC)	16.0.1
2019-09	SA#85	SP-190689	0017	1	A	Additional Critical Assets and Threats to PGW Annex R16	16.1.0
2019-09	SA#85	SP-190688	0019	1	B	UDM critical assets and threats to TR 33.926	16.1.0
2019-09	SA#85	SP-190688	0020	1	B	AUSF critical assets and threats to TR 33.926	16.1.0
2019-09	SA#85	SP-190688	0021	1	B	Adding SEPP critical assets and threats to TR 33.926	16.1.0
2019-09	SA#85	SP-190688	0022	1	B	Adding NRF critical assets and threats to TR 33.926	16.1.0
2019-09	SA#85	SP-190688	0023	1	B	NEF critical assets and threats to TR 33.926	16.1.0
2019-09	SA#85	SP-190688	0024	1	B	Adding critical assets and threats for general NFs to TR 33.926	16.1.0
2019-09	SA#85	SP-190688	0025	1	B	Adding SMF related critical assets and threats to TR 33.926	16.1.0
2019-09	SA#85	SP-190688	0026	1	B	Assests and threats specific to the AMF	16.1.0
2019-09	SA#85	SP-190688	0027	1	B	Adding UPF related critical assets and threats to TR 33.926	16.1.0
2019-12	SA#86	SP-191138	0029	-	D	Miscellaneous Editorial clarifications	16.2.0
2019-12	SA#86	SP-191138	0030	-	F	Clarification on aspects specific to the network product class UDM and AMF	16.2.0
2020-03	SA#87E	SP-200139	0031	1	B	Adding a clause of Threats related to key reuse for the eNB	16.3.0
2020-03	SA#87E	SP-200136	0032	1	F	Updating the clause of Key Reuse for the gNB	16.3.0
2021-03	SA#91e	SP-210117	0039	1	F	Clarification on exposure of confidential IEs in N32-f message in TR 33.926	16.4.0
2021-03	SA#91e	SP-210117	0037	1	B	Threat to send EAP-Identity Request by N3IWF	17.0.0
2021-06	SA#92e	SP-210445	0041	1	B	Adding asset, description and threats to TR 33.926 for NWDAF SCAS	17.1.0
2021-06	SA#92e	SP-210447	0044	1	B	IMS SCAS: living doc for the threats	17.1.0
2021-06	SA#92e	SP-210440	0045	-	B	CR to add threat related to R-16 features of network products to 33.926	17.1.0
2021-09	SA#93e	SP-210847	0046	1	F	Add threat to TR 33.925	17.2.0
2021-09	SA#93e	SP-210848	0048	-	B	SCAS_5G_IPUPS: New threats to IPUPS to TR 33.926	17.2.0
2021-12	SA#94e	SP-211387	0049	-	B	New Annex with Assets and Threats specific to SCAS SCP	17.3.0
2021-12	SA#94e	SP-211371	0050	-	B	Minimum set of functions for SCP	17.3.0
2022-06	SA#96	SP-220546	0058	-	A	Correction on clause F.2.1 in TS 33.926	17.4.0
2022-06	SA#96	SP-220547	0059	-	F	Delete Threat Analysis on Finding the right NF instance are serving the UE	17.4.0
2022-06	SA#97e	SP-220887	0061	-	A	Proposed correction to Annex D on gNB network product class	17.5.0
2022-12	SA#98e	SP-221148	0063	-	A	Correction to the gNB threats in TR 33.926	17.6.0
2023-06	SA#100	SP-230597	0069	1	A	Correcting some references in TS 33.926	17.7.0
2023-09	SA#101	SP-230903	0078	-	F	Addition of critical assets and threats specific to NSSAAF network product class	17.8.0

History

Document history		
V17.3.0	May 2022	Publication
V17.4.0	July 2022	Publication
V17.5.0	September 2022	Publication
V17.6.0	January 2023	Publication
V17.7.0	July 2023	Publication
V17.8.0	October 2023	Publication