ETSI TR 133 926 V15.1.0 (2018-09)

LTE;
Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
(3GPP TR 33.926 version 15.1.0 Release 15)

Reference
RTR/TSGS-0333926vF10

Keywords
LTE,SECURITY

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://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".

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.

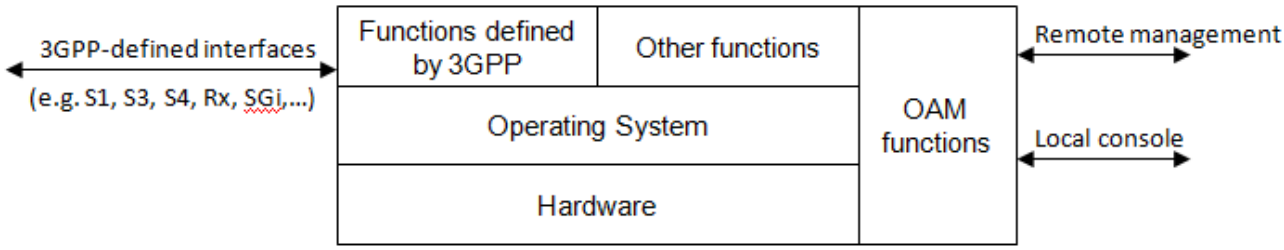

Figure 4.3-1: GNP model

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 requirement:

NOTE: Although the present document intends to cover the security problems and security requirements for all NP functions described in the versions of 3GPP specifications, what other NP, in additional to the MME, 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 is 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 an unsalted hashes is 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 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 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 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 for another source (e.g. USB flash drive, memory card), the GNP bootloader may maliciously 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, without 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 disclosure 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 asset.

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:
  - A 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 asset.

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 asset.

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 asset.

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 asset.

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 comprise the integrity of RRC signalling and make possible Man in the Middle attacks in the AS domain and intercept, for example, the 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 has been 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 it 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 because part of a software distribution. Consequently there might be the risk that an attacker enables these applications without the 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, function 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 uses 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 and result 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 an 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 extra 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 executing 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

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 to contain MME application, a set of running processes (typically more than one) executing the software package for the MME functions and OAM functions that is 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].

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 [8].

A.2 Assets and threats specific to the MME

A.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 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 correct, 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 thee 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 is 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 [AA].

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 24.401, Release 8 [8].

B.2 Assets and threats specific to the PGW

B.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 eNB to be protected are:

- PGW Application;
- UE data: UE usage and charging data e.g. subscriber's identities (e.g. IMSI), packet count, etc.
- 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 uses), including User account data and credentials, Log data, configuration data, OS files, PGW application, Mobility Management data 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 with data
- *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 misoperations (e.g. mischarging) will be executed on UEs.
- *Threatened Asset: TBA*

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 with data, DoS
- *Threat Description*: If the destination address of uplink packets sent by a UE is other 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 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: TBA*

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, Resource exhausion
- 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

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 to contain eNB application, a set of running processes (typically more than one) executing the software package for the eNB functions and OAM functions that is 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 [AA].

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 3GPP TS 36.300, Release 8 [BB] and clause 4.4.1 of 3GPP TS 24.401, Release 8 [8].

C.2 Assets and threats specific to the eNB

C.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 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.
- 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. Where, any active attacker can perform masquerading by making use of the legitimate users' UE identifiers to gain access to the network. This threat scenario assume 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 leads to denial of service to legitimate users. This threat scenario assume 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 assume 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 handles 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 assume that the S1, X2 reference points are not within the security environment

- *Threatened Asset:* Sufficient Processing Capacity

Annex D:
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

History

Document history		
V15.1.0	September 2018	Publication