**3GPP TSG-SA3 Meeting #107-e *S3-221171***

**e-meeting, 16 - 20 May 2022 *revision of S3-220983***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **TR 33.926** | **CR** | **draftCR** | **rev** | **<Rev#>** | **Current version:** | **17.3.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Addition of critical assets and threats specific to MnF network product class |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_MF |  | ***Date:*** | 2022-05-16 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | In order to complete the work on the Security Assurance Sepcification (SCAS) for the Management Function (MnF) as for any other function, it is required to add a dedicated annex in 3GPP TR 33.926 including a network product class description with the corresponding critical assets and threats in accordance to a pre-established template.  |
|  |  |
| ***Summary of change:*** | Addition of a new annex including the critical assets and threats pertaining to the MnF network product class |
|  |  |
| ***Consequences if not approved:*** | Incomplete security assurance work for the Management Function (MnF) |
|  |  |
| ***Clauses affected:*** | 2, 3.2, 4.3, 4.4, Annex X (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This draftCR's revision history:*** | SA3#106e: S3-220524, S3-220526SA3#107e: S3-220885, S3-220886-r1, S3-220887-r1, S3-220888-r1 |

\*\*\*\* Start of Changes\*\*\*\*

# 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*.

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

[x] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[y] 3GPP TS 28.530: "Management and orchestration; Concepts, use cases and requirements".

\*\*\*\* Next Changes\*\*\*\*

## 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

MnF Management Function

OAM Operation and Management

NP Network Product

BSS Business Support System

AAA Authentication, Authorization, Account

TN Transport Network

\*\*\*\* Next Changes\*\*\*\*

## 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.

NOTE: Functions defined by 3GPP can be network functions and/or management functions.

### 4.3.3 Other functions

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

### 4.3.x OAM functions

OAM function provide capabilities to support OAM protocols and perform operation and management on the network product.

 NOTE 1: OAM function are management functions defined by 3GPP. For example, a network product (NP) for 3GPP defined RAN/CN network function (NF) may include a embedded management function (MnF) defined by 3GPP for operation and management of the RAN/CN NF.

### 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) or other management functions.

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

**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.

\*\*\*\* Next Changes\*\*\*\*

## 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:

- Non 3GPP defined management functions to support remote OAM.

- Management functions to support local OAM.

### 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.

\*\*\*\* Next Changes\*\*\*\*

***All the text below is new. Since this is the living document, the baseline is shown without revision marks for convenience when writing new contributions to this document.***

Annex X:
Aspects specific to the network product class MnF

# X.1 Network product class description for the MnF

## X.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 MnF network product class.

A 5G MnF NP implement 3GPP-defined functions from various releases. As specified in TS 23.533 [x], a 5G MnF may support management services such as for performance management, configuration management or fault supervision services, etc.

By comparison to the Figure 4.3-1 (GNP model), a 5G MnF NP includesfunctions defined by 3GPP, other functions, operating system and hardware. According to clause 5.3 of TS 28.533 [x], there are two types of MnFs : cross domain MnF and domain MnF. Figure XX.1.1-1 shows MnF NPs as blackbox and typical interfaces supported by the both types of NPs These MnF types differ slightly in the types of interfaces they support as explained below.

The generic interfaces supported by both MnF NP classes are interfaces for remote management, local console, towards digital portal, to central AAA, to MnF in other domain. The cross domain MnF specific interfaces are interfaces towards external consumer, towards BSS, to TN management system. The domain MnF specific interfaces are interfaces to NF in the same domain.

## X.1.2 Minimum set of functions defining the MnF 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 MnF network product class, it is necessary to define the common set of 3GPP-defined functionalities that is constitutive for a MnF. As part of the MnF network product, it is expected that the MnF contains MnF application, a set of running processes (typically more than one) executing the software package for the MnF functions and OAM functions that are specific to the MnF network product model. Functionalities specific to the MnF network product introduce additional critical assets and/or threats as described below. Related security requirements and test cases have been captured in TS 33.526 [x].

Note: For the purposes of the present document, this common set is defined to be the list of functions contained in TS 28.533 [y], TS 28.530 [z].

# X.2 Assets and threats specific to the MnF

## X.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 MnF to be protected are:

* MnF Application
* The interfaces of MnF to be protected and which are within SECAM scope: for example
	+ External Client access interface
	+ Interface between MnF and NF
	+ Interface between RAN/CN MnFs and Cross Domain MnFs
	+ Interface between MnF and AAA infrastructure, if any
	+ Service based interfaces, if any
* Management data: User account data, Performance data, Fault supervision data, Configuration data, Log data, etc.

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

## X.2.2 Threats related to MnF assets

### X.2.2.1 Over-Privileged Data Processes

* *Threat name:* Over-Privileged Data Process
* *Threat Category*: Tampering of Data, Elevation of privilege
* *Threat Description*: If the MnF product does not evaluate the user privilege for access to data or can allow an attacker to obtain elevated priviledges, an attacker may operate the data with low privilege, this kind of mis-operation not only impacts on the MnF itself, but also the NFs that the MnF connects to.
* *Threatened Asset*: Management data

\*\*\*\* End of Changes\*\*\*\*