**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220150-r1***

**e-meeting, 14 - 25 February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **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 | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Revise generic network product to support management function |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_MF |  | ***Date:*** | 2022-01-30 |
|  |  |  |  |  |
| ***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:*** | The existing Security Assurance Specification (SCAS) defined in 3GPP is focused 3GPP defined network function (NF), 3GPP defined management function (MnF) is not well considered. The CR proposes to revise the specification to adapt 3GPP defined MnF as well.  |
|  |  |
| ***Summary of change:*** | 1. Extend Generic Network Product (GNP) model to cover 3GPP defined management function. 2. Revise scope of the document to reflect 3GPP defined MnF. |
|  |  |
| ***Consequences if not approved:*** | The security assurance of 3GPP defined management function cannot be tested and evaluated in standardized way. |
|  |  |
| ***Clauses affected:*** | 4.3.2, 4.3.3, 4.3.6, 4.3.x (new), 4.4.3 |
|  |  |
|  | **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:*** | Input for Living document of TS 33.926 for SCAS\_5G\_MF (S3-220186 ) |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF 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 can be management functions defined by 3GPP or other functions. 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.

 NOTE 2: Other non-3GPP defined OAM functions may include functions to support management of operation system, hardware or other 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) 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.

## 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES