**3GPP TSG-SA3 Meeting #115 *S3-240860***

**Athens, Greece, 26th Feb 2024 - 1st Mar 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.926** | **CR** | **0086** | **rev** | **3** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at  http://www.3gpp.org/Change-Requests.* | | | | | | | | |
|  | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Annex regarding assets and threats specific to the PCF network product class | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | BSI (DE) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_PCF | | | | |  | ***Date:*** | | | 2024-02-16 |
|  |  | | | |  | |  | | |  |
| ***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 can be found in 3GPP TR 21.900. | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to the work item SCAS\_5G\_PCF and the discussion paper (S3-240015), the PCF is associated with certain threats. However, these threats are not included in TR33.926. This leaves a blind spot on the threat associated with the PCF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add an annex of threats related to the PCF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | If this change is not accepted, the testers executing the SCAS test cases will be unclear about the consequences of failing test cases and the threats associated with the PCF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 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 CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

# 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] Void

[27] 3GPP TS 33.522: "5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)".

[28] Void

[29] 3GPP TS 38.300: "NR; NR and NR-RAN Overall Description; Stage 2".

[30] 3GPP TS 38.401: "NG-RAN; Architecture description".

[31] 3GPP TS 23.501: "System Architecture for 5G System; Stage 2".

[32] 3GPP TS 33.523: "5G Security Assurance Specification (SCAS); Split gNB product classes".

[33] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[34] 3GPP TS 28.530: "Management and orchestration; Concepts, use cases and requirements".

[35] 3GPP TS 33.526: "Security Assurance Specification for the Management Function (MnF)".

[36] 3GPP TS 33.537: "5G Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF)".

[37] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[38] 3GPP TS 33.326: "Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class".

[39] 3GPP TS 33.528: "Security Assurance Specification (SCAS) for Policy Control Function (PCF)".

### \*\*\*\*\*\*\*\*\*\* END OF CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

Annex X:   
Aspects specific to the network product class PCF

# X.1 Network product class description for the PCF

## X.1.1 Introduction

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

## X.1.2 Minimum set of functions defining the PCF network product class

As part of the PCF network product, it is expected that the PCF to contain PCF application (for data analysis), a set of running processes (typically more than one) executing the software package for the PCF functions and OAM functions that is specific to the PCF network product model. Functionalities specific to the PCF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.528 [39].

NOTE: For the purposes of the present document, this common set is defined to be the list of PCF functions contained in clause 6.2.4 of 3GPP TS 23.501 [8].

# X.2 Assets and threats specific to the PCF

## 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 PCF to be protected are:

- PCF Application;

- PCF context Data: i.e. subscriber's identities (SUPI),

- The interfaces of PCF to be protected and which are within SECAM scope:

- Service based interface, Npcf, for providing services for AMF, SMF, NWDAF, NEF, CHF, TSCTSF, AF, and 5G DDNM

- Service based interface for consuming services from UDR

- Console interface, for local access: local interface on PCF

- OAM interface, for remote access: interface between PCF and OAM system

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

- PCF Software: binary code or executable code

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

### \*\*\*\*\*\*\*\*\*\* END OF CHANGE \*\*\*\*\*\*\*\*\*\*