**3GPP TSG-SA3 Meeting #114e *ad-hoc S3-240XXX***

Electronic meeting, online, 22 - 26 January 2024

**Source: Federal Office for Information Security (BSI Germany)**

**Title: Discussion on PCF-Specific SCAS Test Cases**

**Document for: Discussion/Agreement**

**Agenda Item: 4.1.1**

# 1 Decision/action requested

***This contribution discusses the possibilities of PCF-specific SCAS test cases.***

# 2 References

[1] 3GPP TS29.513 Policy and Charging Control signalling flows and QoS parameter mapping

[2] 3GPP TS29.514 Policy Authorization

[3]   3GPP TS29.534 Access and Mobility (AM) Policy Authorization

[4]   3GPP TS29.507 Access and Mobility (AM) Policy Control

[5]   3GPP TS29.501 Background Data Transfer (BDT) Policy Control

[6]   3GPP TS29.523 Policy Control Event Exposure

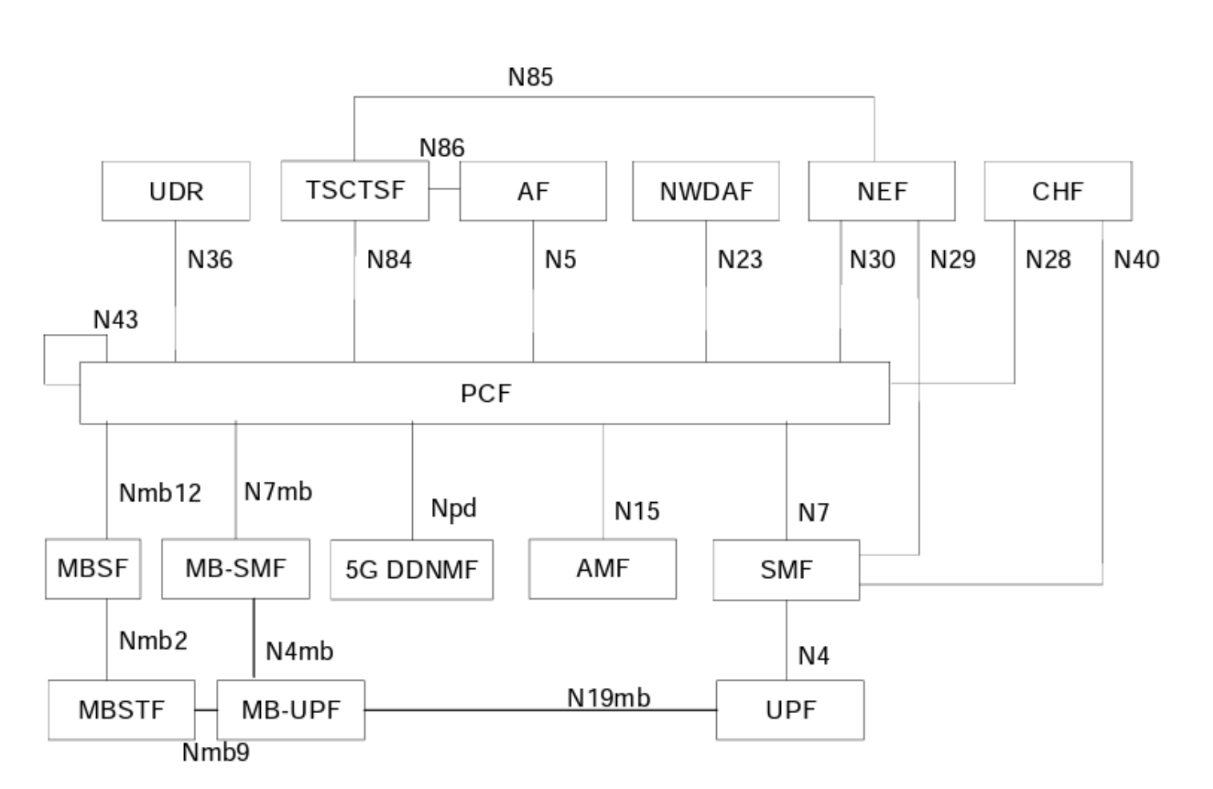
[7]   3GPP TS29.525 UE Policy Control

[8] 3GPP TS33.528 Security Assurance Specification (SCAS) for Policy Control Function (PCF)

[9] 3GPP TR 33.916, Security Assurance Methodology (SECAM) for 3GPP network products

# 3 Rationale

The PCF plays a vital role in the security procedure by controlling and maintaining various security-relevant policies in the 5G SA network. SCAS\_5G\_PCF aims to study the role of PCF security requirements in the 5G core network and examines attempts for specific SCAS test cases regarding the PCF network function. Hence, the PCF has interfaces with numerous consuming and a handful of providing network functions, as illustrated below.



Of particular interest are the following Interface definitions:

* Policy and Charging Control signalling flows and QoS parameter mapping [1]
* Policy Authorization [2]
* Access and Mobility (AM) Policy Authorization [3]
* Access and Mobility (AM) Policy Control [4]
* Background Data Transfer (BDT) Policy Control [5]
* Policy Control Event Exposure [6]
* UE Policy Control [7]

During the analysis, it became apparent that the PCF performs a maintenance function. This means that policies are stored and received by a similar network function type (NFType). For instance, the AM Policy Authorization and AM Policy Control functions are specifically designed for use by the AMF. With this in mind, we have considered two attacker models. The first model involves an attacker who has direct access to the PCF, the second uses a network function with PCF access as an intermediate node.

For the first case, the attacker must be a network function with access to the PCF via one of the mentioned network interfaces. However, this type of attack is prevented by the security definitions in 33.501. Since these requirements are not exclusive to the PCF, they are already reflected in the general SCAS test cases of 33.117.

In the second scenario, the attacker has access to network functions that can reach the PCF. However, we assume that the network function that accesses the PCF operates correctly. This assumption shifts the responsibility to those network functions, which must be implemented and tested properly (via SCAS).

Therefore, at this time, we were not able to identify any specific test cases for the PCF.

Recommendations:

(R1) No specific test cases for the PCF shall be included in the 3GPP TS33.528 [8]

# 4 Detailed proposal

Regarding the analysis outlined in the Rationale above, BSI's proposal is to agree on the current PCF SCAS (TS 33.528 V0.3.0) as being 80% ready and thus version v18.1.0 of PCF SCAS (without specific test-cases, using references to TS 33.117 alone).