**3GPP TSG-SA2 # 146E (e-meeting)S2-21xxxxx**

**August 16 – August 27, 2021**

**Source: Orange**

**Title: Discussion on data collection via SCP activity exposure**

**Document for: Discussion**

**Agenda Item: 9.1.3**

**Work Item / Release: Rel-18**

***Abstract of the contribution:*** *This paper discusses on the possibility to use the SCP as a source for collecting targeted events concerning certain UEs or NFs and proposes an objective to be added to the Rel-18 eNA study.*

# Discussion

The 5G SBI Service Communication proxy is a privileged point of exchange between NFs in the network. However, as the SCP is not an NF, it does not offer event exposure services.

An SBI event consists of HTTP headers, Request URI, and various JSON or binary bodies.

* The Request URI indicating the resource concerned (UE and type of service)

Request URI: {apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>

* The HTTP protocol uses basic HTTP headers, but also various specific 3GPP headers.
* To perform its SBI routing operations, the SCP also performs JSON body part parsing using implementation-dependent techniques.

It is proposed to investigate the possibility of collecting SBI traffic (activity exposure) in a targeted manner by having a protocol for interrogating the SCP. This protocol would allow, with the help of appropriate filters, to target specific NFs or UEs, on all or part of the exchanged requests.

The potential benefit of having activity exposure mechanisms by the SCP would be:

a. To obtain a global view of signalling traffic (general outages, busy hours).

For example, traffic statistics could be compiled according to the type of service and requests, the coverage area of a NF. This would in particular compensate for the lack of OSS standardisation on SCP.

b. To provide an alternative means of exposing UE activities on several NFs. This would make it possible to overcome the deficiency of a data exposure mechanism of an NF (implementation) or of a type of NF (exposure not yet standardised), or to supplement it. This could be a mechanism of intermediate complexity between NF Event Exposure and simple tapping, which generates a lot of signalling traffic. On the contrary, being able to express filters would reduce the exposure of the activity to a limited number of EUs, applications, NFs, etc.

Typical use cases among eNA analytics would be, for example:

- clustering of a UE by analysing the frequency of queries

- detecting of abnormal behaviour

- measuring of the load of an NF

- measuring the load of a Slice

- detecting UE behaviour (location, communications) with the addition of specific headers or deep analysis of JSON

# Conclusion and Proposal

The SCP can offer data collection services as a complement/alternative to the exposure services offered by some NFs.

It is proposed to investigate whether the SCP could expose data to the NWDAF via a specific reference point.

The study would involve the following aspects.

1. Exposure scenarios:
	1. global view of traffic, exposure of UE activities
	2. Suitability for eNA use cases (NWDAF)
	3. Dependency on SCP modes (with or without discovery delegation)
2. Exposure mechanisms
	* Subscription and filtering mechanisms: HTTP2 level criteria (Request URI, existing headers (e.g. 3gpp-sbi-correlation-info defined in TS 29.500), new headers, or more or less partial application level (DPI-like) (e.g. on some JSON key fields).
	* Access interface and protocol: via CN (SBI), via OSS API
	* For UE activity monitoring: partial or total parsing (body) of the request (including JSON data).
3. Impact on SCP load.

We propose to add this as an objective to the Rel-18 Study Item following up on eNA\_ph2.