**3GPP TSG-SA3 Meeting #113 *S3-23xxxx***

**Chicago, USA, 6 - 10 November 2023** **(revision of xx-yyxxxx)**

**Source: Huawei, HiSilicon**

**Title: New SID on 5G Security Enhancement for NEF**

**Document for: Approval**

**Agenda Item: 6**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on 5G Security Enhancement for NEF

Acronym: FS\_NEF\_Sec

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-19

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | X |  |
| No | X | X | X |  |  |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
|  |  |  |  |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text} |

**Dependency on non-3GPP (draft) specification:**

{This section is to be typically used to identify the IETF dependencies. Delete the header "Dependency on non-3GPP (draft) specification:" if no such dependency}

# 3 Justification

Currently, the NEF Northbound interface is specified between the NEF and the AF, which allows the AF to access the services and capabilities provided by 3GPP network entities. The authorization in NEF is specified in clause 12.4 in TS 33.501 where it is stated that after the authentication, NEF determines whether the AF is authorized to send requests to the target NF. In addition, the NEF is required to authorize the requests from the AF using OAuth-based mechanism according to the provisions given in RFC 6749.

Unlike to how the use of OAuth token was profiled for SBA in TS 33.501 or for CAPIF in TS 33.122, the related requirement for NEF remains at a high level. The mapping of role and network entity is not explicitly defined. The authorization grant used for NEF is not clear. Currently, there are four options (including authorization code, implicit, resource owner password credentials, client credentials) on the table. In addition, RFC 6749 only specified the authorization framework. The details for using OAuth 2.0 (e.g. the extent provided by the authorization token) are missing. The topic of NEF authorization has also been debated in several past studies for specific features. Such related discussions can be grouped as AF-level authorization, Service-level authorization, and Resource-level authorization, which depends on the authorization granularity level. To avoid repeated discussion, it will be beneficial to summary the common authorization requirement and potential solutions which can be used for multiple use cases.

In addition, from the current specifications the types of Application Functions (e.g., trusted, untrusted, in operator domain, outside operator domain) considered by 3GPP is not clear and so correspondingly this makes the expected security properties, requirements for these Application Functions unclear. Moreover, the security mechanisms for the interaction between the network and these Application Functions are unclear. i.e., there are no clear definitions and security requirements for types of Application Functions which are the consumers of the Network Exposure Functions. Without any clear definition and security requirements, for example, an untrusted AF can behave like a trusted AF to access sensitive information although it is not authorized. While in TS 33.501 the term "3GPP operator domain" is used without any clear definition, in TS 23.501 "trust domain" term is used without having any impact on security handling. Therefore, there is no alignment between these two terms. More details about the need of clearer and security-gap-free specification for exposure security is given in the endorsed discussion paper S3‑220542.

# 4 Objective

The objectives of this study are to identify key issues, potential security requirements and solutions with respect to Rel-19 enhancement for NEF. Specifically:

* Identify the additional security threat and requirement for network explore services in NEF.
* Study the details (e.g. role, authorization grant, the extent provided by the authorization token) for using OAuth 2.0 in the authorization of AF’s requests.
* Clarify the granularity of authorization and study the solutions, which are applicable for all or multiple use cases.
* Studying boundaries of the 5GC in technical terms, studying more concrete definitions of the terms "3GPP operator domain" and "trust domain" (specifically wrt. external capability exposure) respectively in TS 33.501 and TS 23.501, considering technical definitions, identifying the relation between these terms, solving the misalignment if exists, and investigating whether new terms are necessary.

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| Internal TR | 33.xyz | Study on 5G Security Enhancement for NEF | TBD | TBD | TBD |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Architecture aspects are for SA2 to study.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Huawei |
| HiSilicon |
|  |
|  |
|  |
|  |