**3GPP TSG-SA3 Meeting #115 *S3-240490***

**Athens, Greece, 26th February -1st March 2024** **(revision of xx-yyxxxx)**

**Source: Huawei, HiSilicon**

**Title: New SID on NEF–AF Exposure Security Enhancement**

**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 NEF – AF Exposure Security Enhancement

Acronym: FS\_EXSEC\_ENH

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 |  |  |  |  | X |

# 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) |
| N/A | N/A | N/A | N/A |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| N/A | N/A | N/A  |

# 3 Justification

Exposure is one of the very important surfaces to access the 3GPP system from outside and should offer a needed set of capabilities, depending on the relation (including level of trust) between the external AF and the CSP. Naturally, it is also a very attractive surface for attackers. A successful attack via an exposure surface may lead to very critical results such as leaking subscribers' or MNO sensitive information to attackers or preventing services to subscribers.

Currently, the NEF Northbound interface is specified between the NEF and the AF for network exposure, 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 defined in RFC 6749.

Although 3GPP network exposure is very critical, there seem to be some security gaps in 3GPP specification because of unclear or underspecified points, and some missing concrete security requirements. Moreover, the specification seems to group Application Functions into only two types (trusted and untrusted) with no intermediate types thus making the specification inflexible. In certain points in the specification, an untrusted AF may also be referred to as a 3rd party AF. However, the technical means associated with these definitions are not clearly specified, therefore leaving room for implementation interpretation. To prevent security attacks from exposure surface (but still allow exposure of essential capabilities depending on the trust level), these gaps are mainly addressed by implementation specific methods. However, implementation specific approaches may create interoperability issues. The best way to ensure both a security-gap-free and interoperable 3GPP network exposure specification is to fill this gap in 3GPP specification by addressing the missing points, making the specifications clearer and resolving misalignments between different specifications.

To have a more concrete picture about the underspecified security mechanism for NEF, a comparison with the SBA and CAPIF can be given. 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, and usage of authorization grant needs more clarification. In addition, RFC 6749 only specifies the authorization framework and leaves the details to the usage, but details of usage of OAuth 2.0 (e.g., the extent provided by the authorization token) is missing in NEF. 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 investigate the unclear aspects of existing specifications with respect to the exposure security, identify key issues, potential security requirements and solutions with respect to Rel-19 enhancement for exposure security. Specifically:

* OAuth2.0 threats as described in RFC 6819 are applicable and impact of these needs to be studied.
* Threats that are mitigated in RFC 8707 and RFC 8705 are applicable.
* ~~Identify the additional security threat and requirement for network explore in NEF. Such as the M~~
* Study respective security measures/requirements to fully specify the security mechanisms including the authentication and authorization with sufficient granularity. Clarify the granularity of authorization and study the solutions, which are applicable for all or multiple use cases.
* 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.
* Study more concrete definitions of the terms "3GPP operator domain" and "trust domain" (specifically with respect to 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.

~~NOTE: CAPIF framework improvement will also be considered for authorization between NEF and AF.~~

TU estimates

Total TU estimates for the study phase: 2 TUs

Total TU estimates for the normative phase: 1 TUs

Total TU estimates: 3 TUs

# 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 | NEF-AF Exposure security enhancements | TSG#104 (Jun 2024) | TSG#105 (Sep 2024) | 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.

SA2, SA6, CT3, CT4 for terminology alignment and security requirement related aspects.

# 9 Supporting Individual Members

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