**3GPP TSG-SA3 Meeting #107-e *S3-220719***

e-meeting, 16 - 20 May 2022 (revision of S3-yyxxxx)

**Source: NTT DOCOMO**

**Title: New SID: Study on SNAAPP securitY: FS\_SNAAPPY**

**Document for: Agreement**

**Agenda Item: 6. New Study/Work item proposals**

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 SNAAPP securitY

Acronym: FS\_SNAAPPY

Unique identifier:

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

Potential target Release: Rel-18

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

## 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) |
| SNA | SA1 | 890024 | Subscriber-aware Northbound API access |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 920014 | Study on application enablement aspects for subscriber-aware northbound API access | SA6 study item defining the architecture of SNAAPP |

# 3 Justification

SA6 is studying in TR23.700-95. application enablement aspects for subscriber-aware northbound API access in CAPIF context The study introduces “resource owner”, e.g. subscriber or user, as an entity capable of granting access to a protected resource and expands the CAPIF API Invoker to include UE applications.

The possible use cases of UE applications acting as API Invokers are:

1. The application on UE triggers an AF, and the AF invokes the northbound APIs (indirect API invocation); and

2. The application on UE directly invokes the northbound APIs (direct API invocation).

When API invocations access protected resources, the invoker AF or UE application needs to be authorized by the resource owner. Given the expected dynamic use cases, a subscriber may need to be able to authorize API invocation in near real time, i.e. at the time of first API invocation.

In order to ensure widespread uptake of this feature by application developers, the authorization framework for SNAAPP will be based on an already widely deployed authorization framework.

In addition, new interfaces discussed in the SA6 study may also need to be secured.

# 4 Objective

Based on SA1 requirements for SNA (TS 22.261 clause 6.10.2) and on the SA6 study (TR 23.700-95), the objective of this study is to:

1. Identify potential new security requirements related to API invocation (such as user authorization) and define potential solutions to fulfil these requirements. Referring to the open issues documented at start of this study, this encompasses:

- Whether and how CAPIF functions can determine the resource owner upon CAPIF invocation

- Whether and how CAPIF can support obtaining authorization from the resource owner

- Whether and how CAPIF can support revocation of authorization by the resource owner

- Whether and how CAPIF can reduce authorization inquiries for a nested API invocation

 The study is not exclusively tailored to CAPIF, but should align with widely deployed authorization frameworks.

2. Identify potential security requirements for APIs used in SNAAPP and define potential solutions to fulfil these requirements.

 This objective includes UE-originated API invocation.

# 5 Expected Output and Time scale

|  |
| --- |
| 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.XXX | Study on security of application enablement aspects for subscriber-aware northbound API access | TSG#97 | TSG#98 | Zugenmaier, Alf; NTT DOCOMO, zugenmai@hm.edu |
|  |  |  |  |  |  |

|  |
| --- |
| 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)

Zugenmaier, Alf, NTT DOCOMO, zugenmai@hm.edu

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

SA1, SA6

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| NTT DOCOMO |
| Convida Wireless |
| ATT |
| Lenovo |
|  |
|  |