**3GPP TSG-SA3 Meeting #115 *draft\_S3-240975-r3***

**Athens, Greece, 26th February - 1st March 2024** **(revision of S3-240704)**

**Source: Samsung**

**Title: New SID on security aspects of CAPIF Phase 3**

**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 security aspects of CAPIF Phase 3

Acronym: FS\_CAPIF\_Ph3-sec

Unique identifier: TBD

Potential target Release: Rel-19

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X |  | X |  |
| No | 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 |
| 960012 | Application enablement aspects for subscriber-aware northbound API access (SNAAPP) | Rel-18 SA6 work item |
| 990048 | Security aspects of SNAPP (SNAAPPY) | Rel-18 SA3 work item |
| 780024 | Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs | SA3 CAPIF specification |
| 1020062 | Study on CAPIF Phase 3 | Rel-19 SA6 study item |

# 3 Justification

SA6 agreed a new study for enhancement of CAPIF Phase-3. In release-18, CAPIF security enhancements were addressed based on SNAAPP requirements. The following security aspects are yet to be addressed.

* Authentication and Authorization between Resource Owner and Authorization Functionality (CCF). For example, authentication and authorization of resource owners, management of service API access granted to the applications (e.g., removal of authorization for some applications to access certain service APIs).
* The security aspects for CAPIF-8 reference point are yet to be specified in TS 33.122.
* Authorization of API invoker(s) which are deployed on the UE accessing resources of other resource owners (users).
* Authorization of granularity of access control based in service operations e.g., restriction of operations for an invoker to perform only fetch operation supported by the service API or based on resources e.g., API invoker can access the same resource provided by multiple service APIs.
* Update of security-related onboarding information without offboarding, since the only way so far is to initiate an offboarding process and then do a new onboarding for renewal of these security parameters.
* Threats as described in RFC 6819 are applicable.
* Threats that are mitigated in RFC 8707 and RFC 8705 are applicable.

Further, industry bodies like Linux Foundation and GSMA are specifying and adopting industry service APIs (e.g., CAMARA, GSMA Open Gateway). Considering the work done in these organizations, any enhancement done in SA6 will require further study in SA3 to align with security aspects or requirements.

# 4 Objective

The objective is to study security enhancement of CAPIF for 3GPP northbound APIs. Ensure that security solutions are aligned with the Rel-19 CAPIF enhancement in SA6.

* WT1: Study the security aspects of CAPIF-8 reference point for authentication, authorization and interactions between Resource Owner and Authorization Functionality (CCF).
* WT2: Study the authorization of API invoker(s) which are deployed on the UE accessing resources of other resource owners (users).
* WT3: Study the authorization for granular access control for service APIs e.g., service operation level, resource level.
* WT4: Study the update of security related onboarding information without offboarding.
* WT5: Study the threat modelling outcome as described in RFC 6819 and its impact.
* WT6: Study security risks mitigated in RFC 8705 and 8707 and its impact on CAPIF.

NOTE : SA3 will need to align with the SA6 on the architecture aspect.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate  (Study) | TU Estimate  (Normative) | SA6 Dependency  (Yes/No/Maybe) | Inter Work Tasks Dependency |
| WT1 | 2 | 1 | Yes | No |
| WT2 | 1 | 1 | Yes | No |
| WT3 | 1 | 0.5 | Yes | No |
| WT4 | 0.5 | 0.5 | Yes | No |

Total TU estimates for the study phase: 4.5

Total TU estimates for the normative phase: 3

Total TU estimates: 7.5

# 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 | TBD | Study on security aspects of CAPIF Phase3 | - | SA#106 (December 2024) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 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

Potential dependency on SA6 aspects.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Samsung |
| Nokia, Nokia Shanghai Bell |
| Ericsson |
| NTT DOCOMO |
| Xiaomi |
|  |