**3GPP TSG-SA WG6 Meeting #62 S6-243355**

**Maastricht, Netherlands, 19th – 23rd August 2024 (revision of S6-243270)**

**Title: LS on CAPIF phase 3 security considerations**

**Response to:**

**Release: Rel-19**

**Work Item: FS\_CAPIF\_Ph3**

**Source:** 3GPP TSG SA WG6

**To:** 3GPP TSG SA WG3

**Cc:**

**Contact person: Walter Featherstone**

[**w\_featherstone@apple.com**](mailto:w_featherstone@apple.com)

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:**

# 1 Overall description

In Rel-19, SA6 is studying potential enhancements to CAPIF (i.e., FS\_CAPIF\_Ph3) in 3GPP TR 23.700.22.

In version 0.4.0 of the TR, seven key issues and twelve solutions have been captured. SA6 would like to draw SA3’s attention to the fact that in several of the key issues (specifically 1, 2, 3, 4 & 6) and solutions (specifically 1, 3, 4, 5, & 12), reference is made to SA3 for security related aspects.

| **KI / Sol** | **KI / Sol title** | **Targeted KI** | **Text extracts referring to SA3 in TR 23.700-22 V0.4.0** |
| --- | --- | --- | --- |
| KI#1 | Managing resource owner consent |  | NOTE: Aspects pertaining to the definition of resource owner consent/authorization over CAPIF-8 are in the scope of SA3, noting that the R18 security aspects of CAPIF supporting RNAA are specified in 3GPP TS 33.122 [3]. |
| KI#2 | Supporting Single Sign-On |  | NOTE: The detailed security aspects related to address Single sign-on (SSO) should be provided by SA3. |
| KI#3 | RNAA architecture enhancements |  | NOTE: The security aspects for the architecture enhancements need to be coordinated with SA3. |
| KI#4 | CAPIF interconnection |  | NOTE: Coordination with SA3 is needed for security details. |
| KI#6 | UE-deployed API invoker accessing resources not owned by that UE |  | NOTE 1: The security aspects need to be coordinated with SA3. |
| Sol #1 | Backend For Frontend | KI#3 | NOTE 2: As noted in clause 6.2.1, security aspects of this solution are not in scope of this specification. However, prior to inclusion of this solution in the normative phase, coordination with SA3 is required on the security considerations and associated procedures for supporting the BFF pattern. |
| Sol #2 | User consent for nested API invocation | KI#1 | Editor's note: The mechanism to ascertain appropriate user consent at the AEF is in scope of SA3. |
| Sol #2 | User consent for nested API invocation | KI#1 | Editor's note: Whether new or enhanced APIs are required in support of this solution is in scope of SA3. |
| Sol #2 | User consent for nested API invocation | KI#1 | Editor's note: Prior to inclusion of this solution in the normative phase, the feasibility of providing a security mechanism to enforce user consent checking at an AEF, which is also aligned with CAPIF RNAA, needs coordination with SA3. |
| Sol #3 | Finer granularity of access control for service API | KI#1 | The coordination with SA3 is needed to align the information flows and procedures in 3GPP TS 33.122 [3]. |
| Sol #4 | CAPIF interconnection | KI#4 | This solution impacts the CAPIF-6/6e interface with new or updated APIs. Security related API(s) will be addressed by SA3. |
| Sol #4 | CAPIF interconnection | KI#4 | NOTE: Security details will be addressed by SA3. |
| Sol #11 | Resource Owner Consent Revocation | KI#1 | NOTE: APIs corresponding to this solution will be specified during normative phase based on SA3 outcome. |

Based on that, SA6 would kindly request feedback on those aspects identified as being in SA3 scope and the following specific aspects:

Key Issue #1: Whether SA3 plan enhancements to assist an AEF in obtaining the purpose of data processing before data processing commences in Rel-19?

Key Issue #2: Whether SA3 plan to provide the security aspects related to address Single sign-on (SSO) in Rel-19?

Key Issue #4: Whether SA3 plan to consider CAPIF interconnection security aspects for AEF service API(s) exposed via CAPIF-6/6e in Rel-19?

Key Issue #6: Whether SA3 plan to lift the restriction that a UE-deployed API invoker can only access resources owned by the user of that UE.

Solution #1: Whether SA3 would consider supporting the BFF patten in Rel-19?

Solution #2: Whether SA3 would consider supporting a security mechanism to enforce user consent checking at an AEF in Rel-19?

# 2 Actions

**To SA3**

**ACTION:** SA6 kindly requests SA3 to provide answers for the questions above.

# 3 Dates of next TSG SA WG 6 meetings

SA6#63 14th October – 18th October 2024 Hyderabad, India

SA6#64 18th November – 22nd November 2024 Orlando, US