**3GPP TSG-SA3 Meeting SA3#115 S3-240969-r2**

**Athens, Greece 26th Feb – 1st March, 2024 (Revision of S3-240710)**

**Source: China Mobile, vivo**

**Title: New SID on Study on security aspects of Core Network Enhanced Support for AIML**

**Document for: Approval**

**Agenda Item: 6**

3GPP™ Work Item Description

For guidance, see [3GPP Working Procedures](http://www.3gpp.org/About/WP.htm), article 39; and [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm).
Comprehensive instructions can be found at <http://www.3gpp.org/Work-Items>

# Title: Study on security aspects of Core Network Enhanced Support for AIML

Acronym: FS\_AIML\_SEC

Unique identifier:

Potential target Release: *{Rel-19}*

# 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 |  |
| No |  |  | x |  |  |
| Don't know | x | x |  |  | x |

# 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

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

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 940084 | Study on Artificial Intelligence (AI)/Machine Learning (ML) for NR Air Interface | Related study for RAN intelligence |
| 940073 | Study on Enablers for Network Automation for 5G - phase 3 | Related study for 5GC intelligence |
| 950021 | Study on security aspects of enablers for Network Automation for 5G - phase 3 | Related security study for 5GC intelligence |
|  |  |  |
|  |  |  |

# 3 Justification

The SA2 Rel-19 AI/ML study is to investigate and identify potential architecture and system-level enhancements to support AI/ML.

Based on the SA2 endorsed document SP-231800 and progress, some objectives are related to security aspects:

- WT#1: Study whether and how to consider enhancements to LCS to support AI/ML based Positioning considering the conclusions in 3GPP TR 38.843.

*Potential security aspect:*

*Based on conclusions in 3GPP TR 38.843 and RAN approved WID RP-234039, 5 use cases (i.e. case 1, 2a, 2b, 3a, 3b) which will be studied by RAN. And as agreed in TR 23.700-84, only case 2b and case 3b (i.e. model is on the LMF) will be studied at this stage, and the main issue is to study model transition between LMF and NWDAF. Thus, the authorization of ML model retrieval should be considered.*

*For case 1 and 2a, the model is located in UE side, and for case 3a, the model is located in gNB side. There is no ML model transition, the only issue may be privacy of collected data, so it is based on RAN conclusion.*

* WT2: Study whether and what potential enhancements are needed to enable 5G system to assist in collaborative AI/ML operation involving 5GC/NWDAF and/or AF for “Vertical Federated Learning (VFL)”. The work will be based only on and limited to the scope of justified use cases.

*Potential security aspect:*

*Authorization of members of VFL group.*

*Security aspects of supporting cross-domain(i.e.5G Core and AF) data transfer for AI model training using VFL, e.g. key exchange among members of VFL group, etc..*

Besides, SA3 has sent LS S3-235110 to SA2 to tell them SA3 has acknowledged the security issue related to the authorization issue of ML model retrieval, and SA3 has not agreed on a solution. Therefore, the authorization issue of ML model retrieval left over from the earlier release should also be studied.

# Objective

**WT#1: Study security aspects on enhancements to LCS to support AI/ML based Positioning considering the conclusions in 3GPP TR 38.843.**

**WT#2: Security aspects of cross-domain (i.e. 5G Core and AF) Vertical Federated Learning**

* WT#2.1 Authorization of members of the VFL group.
* WT#2.2 Security aspects to support VFL, e.g. key exchange among members of VFL group if required for the VFL algorithms.

**WT#3: Study the leftovers from earlier releases, e.g., authorization issue of ML model retrieval**

NOTE: More objectives could be added based on SA2 and RAN’s progress, e.g. security issues derived from WT#1.1, WT#1.2, and WT#1.3 of SP-231800.

**TU estimates and dependencies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe)  | Inter Work Tasks Dependency  |
| WT #1 | 1.0 | 0.5 | Yes | No dependency |
| WT #2 | 2.0 | 1.0 | No | No dependency |
| WT #3 | 1 | 0.5 | No | No dependency |
|  |  |  |  |  |

Total TU estimates for the study phase: 4

Total TU estimates for the normative phase: 2

Total TU estimates: 6

# 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 aspects of Core Network Enhanced Support for AIML | TSG SA#105 (Sept., 2024) | TSG SA#106 (Dec., 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)

.

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

SA2 and RAN for architecture aspects.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| China Mobile  |
| vivo |
| China Telecom |
| Oppo |
| ZTE |
| Apple |
| Interdigital |
| Nokia |
| Nokia Shanghai Bell |
| Lenovo |
| Philips |
| Xiaomi |
| Ericsson |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |