**3GPP TSG-SA3 Meeting SA3#115 draft\_S3-240710-r2**

**Athens, Greece 26th Feb – 1st March, 2024 (Revision of S3-24xxxx)**

**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 |  |  |  |  |  |
| Don't know | x | 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 enhancements .

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

- WT#1: AI/ML cross-domain coordination aspects

- WT1.1 – Study whether and how to support UE data collection to meet requirements for RAN AI support for air interface operation (for RAN) for UE-side model training documented in 3GPP TR 38.843 clause 7.2.1.3.2. This includes identifying what benefit can be achieved from enhanced UE data collection in 5G System, and the potential impacts on the 5G framework, including potential enhancements to policy control and OAM. The WT will also discuss the possible data leakage from the operator’s domain which should be avoided and the network control over data collection.

*Potential security aspect:*

*SA2 study whether and how to enhance UE data collection framework to meet requirements for RAN AI support for air interface operation. In this case, 5GC may collect the UE related data or radio related data from UE or RAN, the authentication,authorization, confidentiality, integrity, availability and privacy of the collected data should be studied in SA3.*

- WT1.2 – Study whether (and how) to support model transfer/delivery to the UE according to RAN1/RAN2 considerations documented in 3GPP TR 38.843 clause 7.1.2.4, including potential enhancements to policy control and OAM. Whether and what entities or functions transfer the AI/ML model or information to the UE will be studied as part of the work. This WT will also discuss the possible data leakage from the operator’s domain which should be avoided.

- WT1.3: Study whether and how to support the alignment of model identification and model management between SA2 and RAN. Work will be based on the possible requirements defined by RAN1 and RAN2 considering the conclusions in 3GPP TR 38.843.

*Potential security aspect:*

*Since AI Model may contain sensitive information (e.g., copyrighted or private) and it may be owned or in custody of vendors or third parties, the authentication, authorization,* *confidentiality and integrity of the model delivery should be studied to see if the UE is authorized to receive the model.*

- WT1.4: 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.*

NOTE 2: Whether SA2 can start work on WT 1.1, 1.2 and 1.3 will be discussed at SA#105 (Sep. 2024) based on the outcome of the related work in the involved RAN WGs(s). Further change in description of WT 1.1, 1.2, 1.3 can be discussed at SA#105.

NOTE 5: security aspects are in the scope of SA3, however architectural aspects related to security enhancements will be discussed in this WT.

*Potential security aspect:*

*It is clear that SA3 will be impacted in this WT 1, but for WT 1.1, WT 1.2 and W 1.3, SA3 should wait for RAN’s progress.*

* 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 selecting the required NF(s) within the 5G Core domain or cross domian(i.e.5GC and AF)in order to collaborate on the VFL operation (i.e. training or inference).*

*Security mechanism of supporting cross-domain(i.e.5G Core and AF) data transfer for AI model training during VFL.*

* WT3: Study enhancements to support NWDAF-assisted policy control and address network abnormal behaviour
* WT3.2 - Study prediction, detection, prevention, and mitigation of network abnormal behaviours i.e. signalling storm with the assistance of NWDAF.

*Potential security aspect:*

*This is a security related objective to use NWDAF assisting security detection, but this part has been studied in ZTS, it need further discussion whether it should be study in this SID.*

SA3 has sent LS S3-235110 to SA2 to tell them SA3 has acknowledged the security issue related to authorization issue of ML model retrieval between MTLF and ADRF, and SA3 doesn’t agree a security solution. So, authorization issue of ML model retrieval between MTLF and ADRF should also be studied if SA3 cannot agree a solution in R18.

# Objective

**WT#1: Security aspects of AI/ML cross-domain coordination**

* WT#1.1 Study support for security aspects of data collection from UE and RAN (Authentication, authorization, integrity, confidentiality, privacy and availability protection,etc..)
* WT#1.2 Study support for security aspects of model transfer/delivery to UE (Authentication, authorization, integrity, confidentiality, privacy and availability protection.etc..)
* WT#1.3 Study support for security aspects on enhancements to LCS to support AI/ML based Positioning considering the conclusions in 3GPP TR 38.843.

NOTE 1: Whether SA3 can start work on WT 1.1 and 1.2 will be discussed at SA#105 (Sep. 2024) based on the outcome of the related work in the involved RAN WGs(s).

**WT#2: Security aspects of Vertical Federated Learning**

* WT#2.1 Authorization of selecting the required NF(s) within the 5G Core domain in order to collaborate on the VFL operation (i.e. training or inference)
* WT#2.2 Security mechanism of supporting cross-domain(i.e.5G Core and AF) VFL.

**WT#3: R18 leftover**

* WT#3.1 Study the authorization issue of ML model retrieval between MTLF and ADRF.

NOTE: More objectives could be added based on SA2 and RAN’s progress.

**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 | Maybe | No dependency |
| WT #2 | 2.0 | 1.0 | Maybe | 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 |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |