**3GPP TSG-SA3 Meeting SA3#113 S3-23XXXX**

**Chicago, US 6th – 10th, 2023 (Revision of S3-23xxxx)**

**Source: China Mobile, Nokia, Nokia Shanghai Bell, Interdigital, AT&T, Apple, Xiaomi, Oppo, Lenovo, Philips, ZTE, Huawei?, Ericsson?**

**Title: New SID on Study on security aspects of AI/ML enhancements**

**Document for: Approval**

**Agenda Item: 6.2**

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 AI/ML enhancements

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 S2-2310034, there are some objectives that related to security aspects:

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

- WT1.1 – Study enhancements to UE data collection framework.

*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 and authorization of the enhanced architecture for UE data collection should be studied.*

- WT1.2 – Study 5GC support for AI/ML model and information sharing with the UE.

*Potential security aspect:*

*SA2 study whether (and how) to support model transfer/delivery to the UE. Since AI Model is sensetive information and it may belongs to vendors, the authentication and authorazation of the model delivery should be studied to see if the UE has the authority to get the model . Also, the 5GC need to have the ability to determin what kind of model can be tranfer to UE, so that data leakage from the operator's domain can be avoided.*

* WT2: Study whether and what potential enhancements are needed to enable 5G system to assist collaborative AI/ML operation involving 5GC/NWDAF or AF for “Vertical Federated Learning (VFL)”.

*Potential security aspect:*

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

*Security mechanism of support cross-domain(e.g. UE, 5G Core, application, OAM) AI model training/inference data transfer*

* 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.Also, NWDAF or NF may exchange data or analytics with OAM(e.g. MDAS) to get the mitigation measures from OAM.*

# Objective

**Objective#1: Security aspects of data collection and Model transfer/delivery to UE**

* Study support for security aspects on data collection from UE and RAN (Authentication, Authorization,Integrity and Confidentiality protection,etc..)
* Study support for security aspects on model transfer/delivery to UE (Authentication, Authorization,Integrity and Confidentiality protection,etc..)

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

* 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)
* Security mechanism of support cross-domain(e.g. UE, 5G Core, application, OAM) AI,ML related data transfer

**Objective#3: Security for NWDAF enhancement**

* Study the security aspects of cyber attack(i.e. signaling storm) prediction, detection, prevention and mitigation
* Study security aspect of abnormal behaviour prediction, detection, prevention and mitigation
* Study the security of information exchange with MDAF,e.g. for digital twin network.

**Objective#4: AI model trustworthiness**

* Study the trustworthiness of AI model, including robustness, reliability and privacy related trustworthiness,etc..

**TU estimates and dependencies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate  (Study) | TU Estimate  (Normative) | RAN Dependency  (Yes/No/Maybe) | Inter Work Tasks Dependency |
| Objective #1 | 1.5 | 0.75 | Yes | No dependency |
| Objective #2 | 1 | 0.5 | Maybe | No dependency |
| Objective #3 | 1 | 0.5 | No | No dependency |
| Objective #4 | 0.5 | 0.25 | 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 AI/ML enhancements | SA#XXX  XXX  2023  (TBD) | SA#XXX  XXX  2023  (TBD) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Nokia |
| Nokia Shanghai Bell |
| Interdigital |
| AT&T |
| Apple |
| Xiaomi |
| Oppo |
| Lenovo |
| Philips |
| ZTE |
| Huawei? |
| Ericsson? |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |