3GPP TSG-SA3 Meeting #106-e *S3-220422r2*

## e-meeting, 14 - 25 February 2022 (revision of S3-yyxxx)

## **Source:** OPPO, Apple, vivo

## **Title:** New SID on Security and Privacy of AI/ML-based services and applications in 5G

## **Document for:** Approval

## **Agenda Item: 4.18**

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 and Privacy of AI/ML-based Services and Applications in 5G

## Acronym: FS\_SPAM

## Unique identifier: *TBA*

## Potential target Release: Rel-18

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X |  | X |  |
| No |  |  | X |  |  |
| Don't know | 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

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) |
|  |  |  |  |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work Items (if any) |
| Unique ID | Title | Nature of relationship |
| 860009 | Study on traffic characteristics and performance requirements for AI/ML model transfer in 5GS | SA1 Release 18 study of use cases and potential performance requirements for 5G system support of Artificial Intelligence AI/ML model distribution and transfer (download, upload, updates, etc.), and identification of traffic characteristics of AI/ML model distribution, transfer and training for various applications, e.g. video/speech recognition, robot control, automotive, other verticals |
| 940071 | Study on 5G System Support for AI/ML-based Services | SA2 Release 18 study focuses on enabling, as defined by SA1 Rel-18 AMMT requirements, TS 22.261, the AI/ML Services & Transmissions with 5GS assistance to support AI/ML model distribution, transfer, training for various applications, e.g. video/speech recognition, robot control, automotive etc. for different types of AI/ML operations |
| 920037 | AI/ML model transfer in 5GS | SA1 AMMT study (AI/ML Model Transfer) in stage-1 is related to how the 5GS supports the transmissions of AI/ML-based services over the application layer.  |

Dependency on non-3GPP (draft) specification: N/A

# 3 Justification

The Stage-1 AMMT study (AI/ML Model Transfer) addresses use cases and performance requirements as to how the 5GS supports the transmissions of AI/ML-based services over the application layer. The study is specifically related to the application layer Artificial Intelligence (AI)/Machine Learning (ML) model distribution and transfer (download, upload, updates, etc.), and identifies traffic characteristics of AI/ML model distribution, transfer and training for various applications, e.g. video/speech recognition, robot control, automotive, other verticals. Current SA3 specifications do not address the secured communications between the UE and the 5G system to supporte device-based application AI/ML tranining, splitting, sharing or inference services, more specificially, how to enable the UE and the 5G system to share sensitive network and user data with each other, respectively. even though some aspect of similar services are specified for the purpose of network automation via the NWDAF at the network level. The Stage-2 FS\_AIMLsys study complements the Stage-1 AMMT study by focusing on 5GS architectural and functional extensions so that service providers can leverage 5GS as the intelligent transmission platform to support AI/ML-based services.

The security aspect of user consentin AI/ML support in 5G is need to be considered in several places. One is that of 5G system allowing certain information on the UE to be transferred to third party applications. Another is user consenting to application layer AI/ML operations on the UE. Additionally user consent may be needed in 5G system assistance for security management (e.g., membership and group management) support for distributed federated learning, splitting, sharing and model distribution which requires data transmission support over 5G system, the security and authorization for third-party application or application functions to take part in application layer AI/ML operations. Potential threat and risks may be introdued to the UE or 5G system due to possible compromise of the application layer AI/ML operation, for example, the split learning mechanism in distributed learning is to enable a group of participants to collaboratively train a deep neural network without sharing their raw data. Not protecting sharing of raw data can lead to compromise of user and UE privacy, especially given the split learning nature of AI/ML operations.

Based on the above considerations, it is important to study the security impacts to 5G system in SA WG3 when supporting 5G AI/ML based services and applications to address any potential security threat as described above.

# 4 Objective

The objectives of this study are to focus on identifying key issues, potential threats, requirements and solutions to enable:

1. 5G system assistance for the security management (e.g., membership and group management) for Distributed/Federated learning, Splitting, Sharing and Model Distribution between application AI/ML endpoints (i.e. UEs and Application AI/ML service/model provider) which requires data transmission support for application layer AI/ML operation over the 5G system

2. The authentication and authorization involving data collection and sharing among UE, AF and the network to take part in application layer AI/ML operation, i.e. UE and network privacy protections to support application AI/ML services over 5G system.

NOTE: Impact of privacy protection is to be coordinated with the study on privacy of over the air identifiers.

3. UE and 5G system to secure AI/ML based services and operations.

4. Secure provisioning of the external parameter required for AI/ML (e.g., expected UE activity behaviors, expected UE mobility, etc.)

Potential normative work will be based on selected security requirements and solutions to address identified threats.

# 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 and Privacy of AI/ML-based Services and Applications in 5G  | TSG#98  | TSG#99 | Marcus Wong, OPPO, marcus.wong@oppo.com |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| N/A | N/A  | N/A  | N/A  |

# 6 Work item Rapporteur(s)

Marcus Wong, OPPO, marcus.wong@oppo.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

SA2 is responsible for the system architectural aspects of AI/ML based services in 5G.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| OPPO |
| Apple |
| vivo |
| Inter Digital |
| Samsung |
| China Mobile |
| Nokia |
|  |
|  |
|  |
|  |