**3GPP TSG-SA3 Meeting #115 AdHoc-e *S3-241311***

**Electronic meeting, online, 15 - 19 April 2024**

**Source: Huawei, HiSilicon**

**Title: New KI on authorization of data access for supporting VFL**

**Document for: Approval**

**Agenda Item: 5.13**

# 1 Decision/action requested

***approve this new KI for inclusion in TR 33.784.***

# 2 References

[1] 3GPP TR 23.700-84, ' Study on Core Network Enhanced Support for Artificial Intelligence (AI)/Machine Learning (ML)'

[2] 3GPP TS 23.288, 'Architecture enhancements for 5G System (5GS) to support network data analytics services', (Release 18).

# 3 Rationale

The SA2 Rel-19 AI/ML [1] study is to investigate and identify potential architecture and system-level enhancements to support AI/ML.

The SA3 Rel-19 FS\_AIML\_SEC study include security aspects of cross-domain (i.e., 5G Core and AF) Vertical Federated Learning.

As description in SA2 Rel-19 AI/ML [1], in a multi-vendor scenario, the VFL would allow participating NWDAF instances to collaborate in VFL without the need for model sharing. It is possible that each participant selects or configures the local model to be used, as such vendor or operator specific local models and features, including not standardized features, are simpler to implement comparing with HFL. There could some necessary information (e.g., gradient, Loss) exchange between VLF participants. The authorization of these data needs to be studied in this release.

# 4 Detailed proposals

SA3 is kindly requested to agree the pCR below to TR 33.784.

\*\*\* BEGINNING OF 1st CHANGES \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[xx] 3GPP TR 23.700-84, ' Study on Core Network Enhanced Support for Artificial Intelligence (AI)/Machine Learning (ML) '.

\*\*\* BEGINNING OF 2st CHANGES \*\*\*

# 5 Key issues

## Editor’s Note: This clause contains all the key issues identified during the study.5.X Key Issue #X: Authorization of VFL data access for supporting Vertical Federal Learning

### 5.X.1 Key issues details

As description in TR 23.700-84 [xx], Vertical Federal Learning (VFL) is a federated learning setting where multiple parties perform training on data sets that share the same sample space but differ in feature space. VFL participants may need to transfer VFL data (e.g., intermediate result, gradients, standard features data, non-standard features, Loss, etc.) when doing VFL. The VFL data may be misused by the other VFL participants and this will pose big security issues, such as label inference Attack, Feature inference Attack, label Model theft.

#### 5.X.2 Security threats

An unauthorized NFc, in principle which is not eligible to retrieve a particular VFL data, could have access to the VFL data.

If there is no protection against accessing VFL data, the data might be misused or distributed to other entities, causing a bigger data security issue.

#### 5.X.3 Potential security requirements

5GC shall support VFL data access authorization for VFL members.

5GC shall support VFL data encrypted when VFL data exchange between VFL members.