**3GPP TSG-SA3 Meeting #120 *S3-251141***

**Athens, Greece 17 – 21 Feburary 2025**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | ***draft*** | **rev** | **-** | **Current version:** | **19.1.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Living document for AIML\_CN\_SEC |
|  |  |
| ***Source to WG:*** | China Mobile, vivo,Huawei, HiSilicon,OPPO,Ericsson,Nokia, Xiaomi |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | AIML\_CN\_SEC |  | ***Date:*** | 2025-2-17 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | This draft CR is the living document for AIML\_CN\_SEC. |
|  |  |
| ***Summary of change:*** | This draft CR is the living document based on the approved WID proposal on Security aspects of Core Network Enhanced Support for AIML. |
|  |  |
| ***Consequences if not approved:*** | Security aspects of Core Network Enhanced Support for AIML will not be supported. |
|  |  |
| ***Clauses affected:*** | X.11 (new clause), X.12 (new clause) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

Start of 1st Change

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC 5G Core Network

5G-AN 5G Access Network

5G-RG 5G Residential Gateway

NG-RAN 5G Radio Access Network

5G AV 5G Authentication Vector

5G HE AV 5G Home Environment Authentication Vector

5G NSWO 5G Non-Seamless WLAN Offload

5G SE AV 5G Serving Environment Authentication Vector

ABBAAnti-Bidding down Between Architectures

AEAD Authenticated Encryption with Associated Data

AES Advanced Encryption Standard

AI/ML Artificial Intelligence/Machine Learning

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

AMF Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF Authentication credential Repository and Processing Function

AUN3 Authenticable Non-3GPP devices

AUSF Authentication Server Function

AUTN AUthentication TokeN

AV Authentication Vector

AV' transformed Authentication Vector

BAP Backhaul Adaptation Protocol

BH Backhaul

CCA Client Credentials Assertion

Cell-ID Cell Identity as used in TS 38.331 [22]

CH Credentials Holder

CHO Conditional Handover

CIoT Cellular Internet of Things

cIPX consumer's IPX

CKSRVCC Cipher Key for Single Radio Voice Continuity

cNRF consumer's NRF

CP Control Plane

CPAC Conditional PSCell Addition or Change

CPA Conditional PSCell Addition

CPC Conditional PSCell Change

cPLMN consumer's PLMN

cRI consumer's RI

cSEPP consumer's SEPP

CTR Counter (mode)

CU Central Unit

DCS Default Credentials Server

DN Data Network

DNN Data Network Name

DU Distributed Unit

EAP Extensible Authentication Protocol

EDT Early Data Transmission

EMSK Extended Master Session Key

EN-DC E-UTRA-NR Dual Connectivity

ENSI External Network Slice Information

EPS Evolved Packet System

FL Federated Learning

FN-RG Fixed Network RG

gNB NR Node B

GUTI Globally Unique Temporary UE Identity

HFL Horizontal Federated Learning

HRES Hash RESponse

HXRES Hash eXpected RESponse

IAB Integrated Access and Backhaul

IKE Internet Key Exchange

IKSRVCC Integrity Key for Single Radio Voice Continuity

IPUPS Inter-PLMN UP Security

IPX IP exchange service

KSI Key Set Identifier

KSISRVCC Key Set Identifier for Single Radio Voice Continuity

LI Lawful Intercept

MBSF Multicast/Broadcast Service Function

MBSSF Multicast/Broadcast Service Security Function

MBSTF Multicast/Broadcast Service Transport Function

MeNB Master eNB

MN Master Node

MO-EDT Mobile Originated Early Data Transmission

MT-EDT Mobile Terminated Early Data Transmission

MR-DC Multi-Radio Dual Connectivity

MSK Master Session Key

N3IWF Non-3GPP access InterWorking Function

NAI Network Access Identifier

NAS Non Access Stratum

NDS Network Domain Security

NEA Encryption Algorithm for 5G

NF Network Function

NG Next Generation

ng-eNB Next Generation Evolved Node-B

ngKSI Key Set Identifier in 5G

N5CW Non-5G-Capable over WLAN

N5GC Non-5G-Capable

NIA Integrity Algorithm for 5G

NR New Radio

NR-DC NR-NR Dual Connectivity

NSSAI Network Slice Selection Assistance Information

NSSAA Network Slice Specific Authentication and Authorization

NSWO Non-Seamless WLAN Offload

NSWOF Non-Seamless WLAN Offload Function

PDN Packet Data Network

PEI Permanent Equipment Identifier

pIPX producer's IPX

pNRF producer's NRF

pPLMN producer's PLMN

pRI producer's RI

PRINS PRotocol for N32 INterconnect Security

pSEPP producer's SEPP

PUR Preconfigured Uplink Resource

QoS Quality of Service

RES RESponse

RI Roaming Intermediary

RH Roaming Hub

SCG Secondary Cell Group

SEAF SEcurity Anchor Function

SCP Service Communication Proxy

SEPP Security Edge Protection Proxy

SCPAC Subsequent Conditional PSCell Addition or Change

SgNB Secondary gNB

SIDF Subscription Identifier De-concealing Function

SMC Security Mode Command

SMF Session Management Function

SN Secondary Node

SN Id Serving Network Identifier

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TLS Transport Layer Security

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TWAP Trusted WLAN Access Point

TWIF Trusted WLAN Interworking Function

TSC Time Sensitive Communication

UE User Equipment

UEA UMTS Encryption Algorithm

UDM Unified Data Management

UDR Unified Data Repository

UIA UMTS Integrity Algorithm

ULR Update Location Request

UP User Plane

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

USIM Universal Subscriber Identity Module

VFL Vertical Federated Learning

XRES eXpected RESponse

End of 1st Change

Start of 2nd Change

X.11 Security for UE positioning based on a ML model at the LMF

X.11.1 General

This clause outlines the security considerations for UE positioning based on a ML model at the LMF. According to TS 23.273 [86], UE positioning based on a ML model at the LMF procedures include data collection procedure and AIML model for positioning retrieval procedure.

Clause X.11.2 outlines the general requirements related to those data collection procedures.

Clause X.11.3 outlines the authorization aspects of LMF retrieval of a trained AI/ML model for positioning.

X.11.2 Security for data collection for the LMF-based AI/ML positioning

Regarding user consent aspect for LMF-based AI/ML model positioning, Annex V of the present document applies.

X.11.3 Authorization of LMF retrieval of a trained AI/ML model for positioning

For authorization of LMF retrieval of AI/ML model for positioning, the security for AI/ML model storage and sharing as described in clause X.10 shall apply.

The NWDAF containing MTLF shall register ML model interoperability ID per LMF-based AI/ML Positioning indication (supporting model training for LMF-based AI/ML Positioning if supported.

The LMF shall register at the NRF including its Vendor ID.

NOTE: How to implement the indication of supporting model training for LMF-based AI/ML Positioning in a backward compatible and extensible manner is up to stage 3.

X.12 Security for Vertical Federated Learning among NWDAFs and AFs

## X.12.1 General

This clause outlines the security considerations for vertical federated learning (VFL) where both AFs and NWDAF can act as VFL participants (i.e. either VFL servers or clients).

The authorization of prospective VFL participants, as described in clause X.12.2, is conducted for NWDAF serves as the VFL server case and external AF acts as the VFL server case.

Clause X.12.3 outlines the general NEF security requirements related to the privacy aspects of VFL.

Clause X.12.4 addresses the protection of communication data used in the VFL process and will reuse SBA security measures as detailed in clause 13.

## X.12.2 Authorization of candidate VFL participants

### X.12.2.1 Authorization of candidate VFL participants for vertical federated learning when NWDAF is acting as the VFL server

Figure X.12.2.x -1 depicts the authorization mechanism for NWDAF as VFL Server. The authorization is based upon the VFL capability information per supported Analytics ID which includes VFL capability type (VFL server and/or VFL client), Analytics ID and VFL Interoperability Indicator per Analytics ID provided by VFL members during registration.



Figure X.12.2.x-1: Authorization of VFL participants (NWDAF Acts as VFL Server)

1. In case of AF as VFL Client, the NEF update its NF profile at the NRF with AF’s VFL capability information per supported analytics ID which includes VFL Capability type i.e. (VFL Client) and VFL interoperability indicator(s) per analytics ID and associated AF ID. NWDAF as VFL Client and NWDAF as VFL Server register its profile as described in clause 5.2 or 6.2H.2.1.1 of TS 23.288[105].

2. The NWDAF as VFL Server discovers VFL Client(s) from NRF by invoking the NFDiscovery\_Request service operation with VFL capability information per supported Analytics ID that includes VFL capability type (i.e. VFL client), VFL interoperability indicator per analytics ID, Analytics ID(s) as specified in clause 6.2H.2.1.1 of TS 23.288[105].

3. The NWDAF as VFL Server sends token request(s) to NRF as specified in clause 13.4.1. The token request(s) includes the Analytics ID, AF ID and optionally VFL interoperability indicator per analytics ID.

4. The NRF checks whether the VFL server NWDAF is authorized to access the NEF and NWDAF (VFL Client) for VFL service(s) by optionally verifying the VFL interoperability indicator in the token request is in the VFL interoperability indicator(s) as received from VFL server and VFL client in Step 1. If the server NWDAF is authorized NRF will issue access token(s) as specified in clause 13.4.1. The token claim may include VFL interoperability indicator for that particular analytics ID, Analytics ID and AF ID.

5. The NRF sends the access token(s) to the NWDAF acting as VFL Server, or rejects the request in case of failed authorization, as described in clause 13.4.1.

6. The NWDAF as VFL Server may send VFLService\_Request to NEF and the token received in Step 5. The service request includes the Analytics ID, AF ID and optionally VFL interoperability indicator per analytics ID .

7. The NEF verify the access token received from the NWDAF. The NEF extract the Analytics ID from the access token and check whether it matches the Analytics ID received in step 6. If the AF ID is included in the token, the NEF also verify that the AF ID matches the AF ID requested in step 6.

8. The NEF sends the VFLService\_Request to the AF (VFL as client) that includes the Analytics ID, AF ID and optionally VFL interoperability indicator per analytics ID. The AF performs authorization of VFL service request based on its local policy and implementation. Protection of NEF-AF interface is as specified in clause 12 of TS 33.501.

9a. The AF sends VFL VFLService response (success or failure) to the NEF.

9b. The NEF forwards the VFLService response to the NWDAF acting as the VFL server.

Editor’s Note: The addition of Internal AF as a server to be covered in the present clause is FFS.

### X.12.2.2 Authorization of candidate VFL participants for vertical federated learning when external AF is acting as the VFL server

Figure X.12.2.2-1 depicts the authorization mechanism for NWDAF as VFL Client and external AF as VFL server. The authorization is based upon the VFL capability information per supported Analytics ID which includes VFL capability type (VFL server and/or VFL client), Analytics ID and VFL Interoperability Indicator per Analytics ID provided by VFL members during registration.



Figure X.12.2.2-1: Authorization of candidate VFL participants for VFL when external AF is acting as the VFL server

1. In case of AF as VFL Server, the NEF update its NF profile as specified in clause 6.2H.2.1.2 of TS 23.288[105], which including AF’s VFL capability information per supported analytics ID which includes VFL Capability type i.e. (VFL Client) and VFL interoperability indicator(s) per analytics ID and associated AF ID. In case of NWDAF as VFL Client it shall register to NRF with its NF profile as specified in clause 6.2H.2.1.1 of TS 23.288[105].

2. The AF sends a Discovery\_Request to the NEF with information Analytics ID, VFL capability type (VFL Client), VFL interoperability indicator to discover for VFL Client. The NEF discovers NWDAF as VFL client from the NRF by invoking the Discovery\_Request as specified in 6.2H.2.1.2 of TS 23.288[105]. The NEF checks based on configured policies whether the AF is entitled to discover service to a VFL client as specified in clause 12 of TS 33.501.

NOTE: Handling of temporary NWDAF instance ID (s) is specified in clause 6.2H.2.1.2 of TS 23.288 [105].

3. The AF acting as VFL server sends VFLService\_Request towards NEF. The Service request shall contain the Analytics ID and optionally VFL interoperability indicator per analytics ID.

4. The NEF request for an access token to the NRF as specified in clause 13.4.1 to perform VFL service towards the VFL clients (NWDAF). The token request shall contain the Analytics ID, AF ID and optionally VFL interoperability indicator per analytics ID.

5. The NRF checks whether NEF is authorized to access the NWDAF for the VFL service(s) by optionally verifying the VFL interoperability indicator in the token request is in the VFL interoperability indicator(s) as received from VFL server and VFL client in in Step 1.

6. If the NEF is authorized, the NRF will issue an access token in response. The token claim may also include VFL interoperability indicator for that particular analytics ID, Analytics ID and AF ID.

7. The NEF send VFLService\_Request to NWDAF (VFL Client) and the token includes the Analytics ID, AF ID and optionally VFL interoperability indicator per analytics ID as token received in Step 6.

8. The NWDAF verifies the received access token as specified in clause 13.4.1 of TS 33.501 and checks for the token claims as received in step 7.

9a. In case of successful access token verification, the NWDAF (VFL as client) sends a VFLService\_Response to the NEF.

9b. The NEF sends the VFLService\_Response to the AF (VFL as Server). Protection of NEF-AF interface is as specified in clause 12 of TS 33.501.

## X.12.3 NEF security requirements

In case that NEF is involved, NF instance ID shall not be transmitted outside the 3GPP operator domain via NEF.

## X.12.4 Protection of communication data used in VFL process.

The current SBA mechanisms as defined in clauses 12.2 and 12.3 of the present document for the NEF-AF interface and clause 13. 1 of the present document for communication among VFL participants shall be used.

End of 2nd Change