**3GPP TSG-SA3 Meeting #115AdHoc-e *draft\_S3-241363-r4***

Electronic meeting, online, 15 - 19 April 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Update procedure for secured and authorized AI/ML model sharing |
|  |  |
| ***Source to WG:*** | Ericsson, Nokia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2024-04-08 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-18 |
|  | *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 proposal is to update the procedure for secured and authorized AI/ML model sharing in order to resolve the NOTE in clause 5.3 in TS 23.288：*NOTE 2: How to authorize an MTLF to request ML models on behalf of an AnLF to another MTLF (e.g., FL server NWDAF) is up to SA WG3.*SA2 has introduced two procedures for ML model request, as described in clause 6.2C.2.2, TS23.288, Thus, the NF service consumer shall extend to both MTLF and AnLF in the authorization procedure in X.10 of TS 33.501 Model producer(MTLF FL Server) needs to check the permission of model consumer(AnLF) when it was represented by another NF service consumer. The security procedure for checking the permission of the ML model consumer is aligned with the procedure for checking permission of the data consumer and DCCF in Annex X.2, where the NF Service Consumer takes the role of the DCCF and the ML model consumer the role of the data consumer. |
|  |  |
| ***Summary of change:*** | It is proposed to introduce a ML model consumer in the procedure of X.10 |
|  |  |
| ***Consequences if not approved:*** |  There is no authorization for the model retrieving procedure defined in TS 23.288. |
|  |  |
| ***Clauses affected:*** | Annex X.10 |
|  |  |
|  | **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:*** |  |

\*\*\* BEGIN CHANGES \*\*\*

# X.10 Security for AI/ML model storage and sharing

The detailed procedure for secured and authorized AI/ML model sharing between different vendors is depicted in Figure X.10-1:



Figure X.10-1: Secured and authorized AI/ML model sharing between different vendors

0a. NF Service producer i.e. NWDAF containing MTLF registers its NF profile in the NRF with ML Model Interoperability indicator per Analytics ID as described in clause 5.2 of TS 23.288 [105]. The ML Model Interoperability indicator is a list of NWDAF providers (vendors) that are allowed to retrieve ML models from this NWDAF containing MTLF.

0b. NF Service consumer e.g., NWDAF registers at the NRF including its Vendor ID, if the NF Service consumer is MTLF, the NWDAF containing MTLF also registers its Interoperability indicator per Analytics ID.

0c. The model is stored in encrypted format unless both the AI/ML model producer (NWDAF MTLF) and storage platform (ADRF) are part of the same system and belong to the same vendor and operator security domain.

 Storage of the model in encrypted format can be required by the trust model established to store and share AI/ML models. The trust model between AI/ML NF producer (NWDAF MTLF), storage platform (ADRF) and NF consumer (e.g., AnLF) is to be determined during the implementation phase among operator and the providers of the different platforms (MTLF, AnLF, ADRF). How the model is encrypted is vendor specific. Key distribution is not specified in this document.

1. If NWDAF containing MTLF determines to store ML model in ADRF, NWDAF containing MTLF triggers the Nadrf\_MLModelManagement\_StorageRequest as described in TS 23.288 [105], optionally including an allowed NFc list. The absence of allowed NFc list indicates that only the MTLF which stored the model is allowed to retrieve the model.

2. ADRF sends the response to NWDAF containing MTLF as described in TS 23.288 [105].

3. NF Service consumer e.g., NWDAF performs Nnrf\_NFDiscovery\_Request operation with the requested Analytics ID to select a suitable NF Service Producer e.g., NWDAF containing MTLF.

In case of the NF service consumer (e.g. NWDAF containing MTLF) request ML models on behalf of another ML model consumer (e.g., NWDAF containing AnLF), before step 3 the ML model consumer (e.g., NWDAF containing AnLF) obtains a token for the analytics ID from NRF same as step 4 which authorizes the ML model consumer to use model retrieval service provided by the NF service consumer and sends the model retrieval service request to the NF service consumer with the Analytics ID, the obtained token, the Vendor ID and the CCA of the ML model consumer.

4a. NF Service consumer e.g., NWDAF requests an access token from the NRF using the Nnrf\_AccessToken\_Get request operation. The token request message contains, besides the parameters described in clause 13.4.1.1.2, the Vendor ID of the NF Service consumer and the Analytics ID. If the NF Service consumer is NWDAF containing MTLF, it also includes its Interoperability indicator per Analytics ID in the request.

In case of NF service consumer request ML models on behalf of another ML model consumer (e.g., NWDAF containing AnLF), the token request message shall also contain the NF instance ID and Vendor ID of the ML model consumer. The NF Service Consumer also includes the CCA of the ML model consumer that it has received in the service request from the ML model consumer.

4b. NRF checks whether the NF Service consumer is authorized to access the requested service in NWDAF containing MTLF. The NRF verifies that the NF Consumer's Vendor ID is included in the NF Service Producer's interoperability indicator for the Analytics ID. If NF Service consumer is a NWDAF containing MTLF, the NRF also verifies that NF Service consumer's Interoperability indicator is subset of the NF Service Producer’s interoperability indicator for the Analytics ID. If the authorization is successful, the NRF grants the token (token1) including the Analytics ID as specified in the clause 13.4.1.

In case of NF Service Consumer request ML models on behalf of another ML model consumer, the NRF also verifies that the Vendor ID of ML model consumer is included in the NF Service Producer's interoperability indicator for the Analytics ID and grants the token(token1) also including the NF Instance ID of ML model consumer in the sourceNfinstanceId IE attribute. The NRF also authenticates the ML model consumer based on one of the SBA methods described in clause 13.3.1.2.

5. NF Service Consumer performs Nnwdaf\_MLModelProvision (Analytics ID, Vendor ID and token1) service operation at the NWDAF containing MTLF to retrieve ML models for the Analytics ID.

In case of NF Service Consumer request ML models on behalf of another ML model Consumer, the Nnwdaf\_MLModelProvision service operation shall also contain the NF instance ID and Vendor ID of the ML model consumer and the CCA of the ML model consumer.

NOTE x: NF Service Producer relies on the NRF to perform the authorization and to check the vendor ID of the NF Service Consumer. The vendor ID cannot be verified by the NF Service Producer.

 6a. The NF Service Producer authenticates the NF Service Consumer and verifies the access token as specified in the clause 13.4.1.1.2 and ensures that the Analytics ID is included in the access token. If verification is successful, NWDAF containing MTLF determines the ML model to be shared for the requested Analytics ID and stored the NF instance ID of NF Service Consumer as part of allowed NF instance list for the ML model.

If the NF Service Consumer request ML models on behalf of the ML model Consumer, the NF Service Producer also authenticates the ML model consumer following clauses 13.3.2 and 13.4.1, and ensures that the ML model consumer is authorized according to the sourceNfinstanceId IE attribute of the access token provided by the NF Service Consumer. The NF Service Producer stores also the NF instance ID of Model Consumer as part of allowed NF instance list for the ML model.

NOTE x: In the case a new ML model consumer comes at a later stage to request the model, which is already available at the NF Service Consumer, steps 4-7 apply. When the request is received by the NF Service Producer (i.e. the model producer), it authenticates the NF Service Consumer and verifies the access token provided along with the service request and sends to NF Service Consumer the access token verification response. NF Service Consumer based upon the response received, either sends the ML model to the ML model consumer or in the case of access token verification failure, the NF Service Consumer rejects the request received by the ML model consumer and does not send the model.

 6b. If the determined ML model is stored in ADRF, and if the NF Service Consumer is not yet in the allowed NFc list stored at the ADRF, the NWDAF containing MTLF triggers the update of Nadrf\_MLModelManagement\_StorageRequest at the ADRF, with NF ID of NWDAF containing MTLF and Model ID, adding the NF Service Consumer to the allowed NFc list. The ADRF verifies that the requesting NWDAF containing MTLF is same as the one that stored the model. Then, ADRF stores the allowed NF instance list for the ML model referenced by the Model ID.

 6c. ADRF sends the response to NWDAF containing MTLF which contains Model ID.

 7. NWDAF containing MTLF sends Nnwdaf\_MLModelProvision Notify to the NF Service Consumer with Model ID, the address of the determined ML model, which can be either the one stored in NWDAF containing MTLF or in ADRF,or ADRF(set) ID. If the address of the determined ML model is provided, steps 8a to 10 are skipped.

 If the ADRF(set) ID is provided, the following steps are applied:

 8a. NF Service Consumer requests an access token from the NRF to be authorized to retrieve the model stored in ADRF as specified in clause 13.4.1.

 8b. NRF verifies that the NF Service consumer e.g., NWDAF is authorized to access the service provided by the ADRF. If verification is successful, NRF grants the token (token2), based on the information provided in ADRF's NF profile.

 9. NF Service consumer e.g., NWDAF requests to retrieve the target model by sending Nadrf\_MLModelManagement\_Retrieval Request as described in clause 10.3.4 TS 23.288 [105], including token2.

 10. ADRF authenticates the NF Service Consumer and verifies the access token (token2) as specified in the clause 13.4.1.1.2. ADRF verifies also the NF Service Consumer’s NF ID is included in the allowed NF instance list for the ML model and/or is same as the NF ID of the MTLF that stored the model. If verification is successful, ADRF sends Nadrf\_MLModelManagement\_ Retrieval Response to the NF Service Consumer, which contains the address of the stored model in ADRF.

 11. NF Service Consumer retrieves the ML model from NWDAF containing MTLF or ADRF based on the ML model file address and decrypts the model per the vendor’s implementation.

NOTE y: As per TS 23.288 [105] clause 10.3.2, how the NF Service Consumer downloads the ML Model is left for implementation.

\*\*\* END CHANGES \*\*\*