**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_S3-230240-r1***

**Electronic meeting, 16 - 20 January 2023**

**Source: Ericsson**

**Title: ENs resolving and evaluation for solution #10**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***It is requested to approve this proposal in TR 33.738.***

# 2 References

[1] 3GPP TR 33.738 v0.4.0 "Study on security aspects of enablers for Network Automation for 5G - phase 3"

[2] 3GPP TR 23.700-81v18.0.0 "Study of Enablers for Network Automation for the 5G System (5GS); Phase 3"

# 3 Rationale

This contribution proposes resolutions for the ENs in solution#10 in TR 33.738 [1] and evaluates the solution.

The following updates and explanations are reflected to resolve the ENs:

* To resolve the following EN, an explanation is added stating that the ADRF provides a one-time URL to the NFp which shares the URL with the NFc after successful authorization so when the ADRF receives the URL from the NFc it ensures that the NFc has been authorized by the NFp.

Editor's Note: Clarification on whether and how this solution addresses the second requirement is FFS.

* The following EN is removed. According to the conclusions in TR 23.700-81 [2], downloading the ML model via URL has been accepted as an option. Also, solutions for privacy issues have been left to SA3 working group. This solution allows the NFp to do further authorization considering ML privacy by proposing usage of vendor ID by the NFp to be able to the authorization based on the vendor of the NFc.

Editor's Note: Alignment with SA2 for the overall procedure and usage of vendor ID is FFS.

* To resolve the following EN, an explanation is added stating that one-time URL is protected using SBA.

Editor's Note: Protection of one-time URLs is FFS.

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

## 6.10 Solution #10: Authorization of AI/ML model sharing between different vendors and usage of one-time URLs

6.10.1 Introduction

This solution addresses key issue # 3 (security for AI/ML model storage and sharing) considering that the consumer (NWDAF containing AnLF) and the producer (NWDAF containing MTLF) can be different vendors.

The second requirement of the key issue is about enabling the ML model storage to ensure that the NFc is authorized by the NFp to retrieve the model. According to this solution, the NFp retrieves a one-time URL from the ADRF and then shares the one-time URL with the NFc. To be able to access to the model, the NFc has to know the one-time URL, which implies that the URL has been shared with the NFc by the NFp after authorization of the NFc by the NFp.

6.10.2 Solution details

The steps of the procedure depicted in Figure 6.10.2-1 are explained below.



 6.10.2-1: Model sharing between NWDAF containing MtLF and NWDAF containing AnLF from different vendors.

Steps:

0a. The NFp registers with the NRF using the interoperability ID. It is assumed that the NRF verifies the vendor ID of the NFp.

0b. The NFc registers with the NRF using the vendor ID. It is assumed that the NRF verifies the vendor ID of the NFc.

Assumption: The NRF can verify the Vendor ID of the NWDAF containing AnLF.

Editor's Note: Alignment with SA2 for the overall procedure and usage of vendor ID is FFS.

Editor's Note: How the NRF verifies the Vendor ID of the NFDAF is pending the resolution of Key Issue #11 NRF validation of NFc for access token requests in TR 33.875 "Study on enhanced security aspects of the 5G Service Based Architecture (SBA)"

0c. The NFp performs some operations for security of the ML model, such as encryption and integrity protection. These operations are out of scope of the solution.

1. If the NFp wants to store the ML model in the ADRF, the NFp triggers storing the ML model in the ADRF. For downloading the model by the ADRF, the NFp provides the address (URL1) of the model in the NFp. Also, the NFp can send the model correlation ID to the ADRF.

2. ADRF securely fetches the protected model. The fetch method and its security are out of scope.

3. The ADRF sends the location of the model (URL2) to the NFp to be used for the NFp to update or access the model in a later point in time.

4. The NFc executes the discovery procedure with the NRF.

5. The NFc request a token from the NRF indicating the analytics ID.

6. The NRF checks whether the vendor ID of the NFc, stored in the profile of the NFc in the NRF, is one of the vendor ID in the interoperability ID in the NFp profile. If the check is successful, then the NRF issues a token that includes the vendor ID of the NFc.

7. The NFc sends the Model request including the token to the NFp.

8. The NFp validate the token and can perform further authorization using the vendor ID specified in the token.

Steps 9 and 10 are executed if the model is stored in the ADRF.

9. After successful authorization, the NFp request a URL, which can be usable only once, from the ADRF.

10. The ADRF checks if the stored model owner is the NFp. If the check is successful, the ADRF provides a URL (URL3) for the stored model. The URL3 can be a URL that is used only once (one time URL).

NOTE: How to provide one time URL by the ADRF is implementation detail which is out of scope of the solution.

11. The NFp provides the URL3 received from the ADRF to the NFc if the model is stored in the ADRF. If the model is stored in the NFp, then the NFp provides the location of the model in the NFp (URL4).

12. The NFc fetches the protected model from the NFp (step 12a) or ADRF (step 12b). The fetch method and its security are out of scope.

13. The NFc performs some operations considering the interoperability ID on the protected ML model such as decryption and integrity check. These operations and keys are out of scope of the solution.

Note that the one-time URL is protected using the current SBA mechanism, so that it cannot be eavesdropped by unauthorized entities. Using one-time URLs further reduces the risk that URLs are leaked and used by unauthorized entities, since the one-time URL will not be valid after the authorized NFp has used it to retrieve the model.

6.10.3 Evaluation

This solution addresses ML model sharing between NFs from different vendors, by allowing the NFp to do further authorization check for model sharing using the vendor id of the NFc. The solution focuses on the ML model downloading via URL case.

**\*\*\*\*** END OF CHANGE **\*\*\*\***