**3GPP TSG-SA3 Meeting #107Adhoc-e *draft-S3-221379-r2***

**e-meeting, 27th June – 1st July, 2022**

**Source: OPPO, Apple**

**Title:** **New solution: Authentication mechanism selection among EEC, ECS, and EES**

**Document for: Approval**

**Agenda Item: 5.9**

1 Decision/action requested

***This pCR proposes to solve the key issue #2.2 by authentication mechanism selection in Edge***

2 References

[1] 3GPP TS 23.558 "Architecture for enabling Edge Applications ".

[2] 3GPP TR 33.739 “Study on security enhancement of support for edge computing phase 2”

[3] 3GPP TS 33.535 "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[4] 3GPP TS 33.222 “Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)”

3 Rationale

This solution addresses security requirement for authentication mechanism selection between EEC and ECS, EEC and EES in key issue #2.2.

It is proposed to realize the authentication mechanism selection between EEC, ECS and EES at the same time with the help of ECS.

The EES Registration procedure allows an EES to provide information to an ECS in order to enable provisioning EES(s) to an EEC as specified in clause 8.4.4 of TS 23.558[1]. Hence, in this procedure, the EES could provide its security capability to the ECS. During the authentication mechanism selection between EEC and ECS, ECS utilizes the capabilities (e.g. UE location) of the 3GPP core network or the profile(s) provided by the EEC to identifies the EES(s) as specified in clause 8.3.3.2 of TS 23.558[1], and helps the EES to select the authentication mechanism based on security capability of EEC and EES.

The ECS provisions Edge configuration information to the EEC which contain the information for establishing a connection with EESs (such as URI), in the Service provisioning procedure as specified in clause 8.3.3 of TS 23.558[1]. The security capability of EES is contained in the Edge configuration information, to establish the security connection between EEC and EES.

4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.739 [2].

\*\*\*\*\*\*\*\*\*\*\* First Change\*\*\*\*\*\*\*\*\*\*\*

6.X Solution #X: Authentication mechanism selection procedure among EEC, ECS, and EES

6.X.1 Solution overview

This solution addresses security requirement for authentication mechanism selection between EEC and ECS, EEC and EES in key issue #2.2.

6.X.2 Solution details

The EEC should be configured with the security capability according to the local configuration (e.g., TLS with AKMA [3], TLS with GBA [4], or other TLS authentication methods). The ECS and EES should be separately configured via network management with mechanisms that are are allowed.

The EES provides the supported authentication mechanism(s) to the ECS during the EES registration procedure in clause 8.4.4.2.2 in TS 23.558[1], and the ECS stores the security capability of the registered EES.

The ECS provisions the Edge configuration information to the EEC which contains the information for establishing a connection with EESs (such as URI), in the Service provisioning procedure as specified in clause 8.3.3 of TS 23.558[1]. ECS helps the authentication mechanism selection between EEC and EES, and contains the selection result in the Edge configuration information, to establish the security connection between EEC and EES.

 

Figure 6.3.X.2-1: Procedure for authentication mechanism selection among EEC, EES, and ECS

Step 0: The EEC is pre-configured with or has discovered the address (e.g. URI) of the ECS.

Step 1. The EEC chooses an authentication mechanism, and sends an Authentication Mechanism Selection Request message to the ECS, including EEC security capability, the chosen authentication mechanism, and may include the UE identifier such as GPSI, connectivity information, UE location and AC profile(s) information. Step 2a. The ECS stores the security capability of EEC, and checks if it supports the authentication mechanism chosen by EEC.

Step 2b. The ECS may utilize the capabilities (e.g. UE location) of the 3GPP core network or the profile(s) provided by the EEC, to identifies the EES as specified in clause 8.3.3.2 of TS 23.558[1]. With the security capability of the identified EES stored in EES registration, and the receiving security capability of the EEC in step 1, the ECS checks if the identified EES supports the authentication mechanism chosen by EEC.

Step3. The ECS sends the Authentication Mechanism Selection Request message to the identified EES, including EEC security capability, and the authentication mechanism chosen by EEC.

Editor’s Note: whether ECS should send the EEC’s security capability and EEC chosen method to EES is FFSStep4. If ECS supports any mechanism in EEC's security capability, ECS may use the authentication mechanism EEC chooses or another mechanism in EEC's security capability (e.g., based on local policy), ECS should sends EEC the Authentication Mechanism Selection completes message including the selection result. Otherwise the ECS should reply with a failure indication.

ECS helps the identified EES to select the authentication mechanism based on the security capability of EEC and EES, and authentication mechanism chosen by EEC, and the selection result of ECS should be contained in the Edge configuration information, and provide to the EEC in the Service provisioning procedure as specified in clause 8.3.2.2 of TS 23.5558[1], for the EEC to establish security connection with the EES. If the EES could not support any mechanism in EEC's security capability, ECS sends a failure indication to EEC.Step5. Upon receiving the Authentication Mechanism Selection Complete message from ECS with the selection result, EEC starts using the mechanism indicated in selection result. Otherwise the authentication mechanism selection failed between EEC and ECS.

6.X.3 Solution evaluation

TBD

Editor’s Note: it is FFS to consider the security capabilities of PLMNs.

Editor’s Note: it is FFS how to solve the authentication selection failure case if there do not exist the same authentication mechanisms.

Editor’s Note: It if FFS to consider the security protection of selection messages between EEC and ECS.

\*\*\*\*\*\*\*\*\*\*\*End of First Change\*\*\*\*\*\*\*\*\*\*\*