**3GPP TSG-SA3 Meeting #109 AdHoc-e Draft\_S3-230208-r1**

**e-meeting, 16th – 20th** **January, 2023**

**Source: OPPO**

**Title: Resolving ENs in Solution #11**

**Document for: Approval**

**Agenda Item: 5.9**

1 Decision/action requested

***Archive the agreement to resolve the Editor’s Notes.***

2 References

[1] S3-230202

3 Rationale

In this meeting, S3-230202[1] is proposed with the following conclusion about default authentication mechanism for KI 2.2:

*“It is concluded that the EEC and EES/ECS shall support the authentication mechanism of TLS with certificates by default, in order to avoid the authentication failure case.”*

If the conclusion was approved, the following ENs can be resolved, since there is a same default security authentication capability at the EEC, ECS and EES.

Editor's Note: How to consider security capabilities of UEs and PLMNs in the negotiation is FFS.

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

4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*START OF CHAGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*

6.9 Solution #11: Authentication mechanism selection procedure among EEC, ECS, and EES

6.11.1 Solution overview

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

6.11.2 Solution details

The EEC should be configured with the security capability according to the local configuration. The EEC should support TLS with certificates by default, and should optionally support TLS with AKMA [3] and TLS with GBA [4]. The ECS and EES should be separately configured via network management with mechanisms that are are allowed the ECS and EES should support TLS with certificates by default and optionally support TLS with AKMA [3] and TLS with GBA [4].

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 6.3.11.2-1: 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 identify 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 FFS

Step4. 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.

6.11.3 Solution evaluation

TBD

In this solution, TLS with certificates is adopted as the default authentication for EEC, ECS and EES.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*END OF CHAGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*