**3GPP TSG-SA3 Meeting #109 AdHoc-e S3-230204**

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

**Source: OPPO**

**Title: Resolving ENs in Solution #9**

**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 and ECS, and the negotiation failure case is avoided.

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 between EEC and ECS.

4 Detailed proposal

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

6.9 Solution #9: Authentication mechanism selection procedure between EEC and ECS

6.9.1 Solution overview

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

6.9.2 Solution details

For authentication between EEC and ECS, EEC and ECS should support TLS with certificates by default, and optionally support TLS with AKMA as specified in TS 33.535 [2] and TLS with GBA as specified in TS 33.222 [3] . And the detail of TLS authentication method selection needs to be addressed.

To support authentication between the EEC and ECS, the EEC and the ECS should be configured with the security capability according to the local configuration (TLS with certificates by default, TLS with AKMA [2] and TLS with GBA [3] optionally supported).

Before the authentication mechanism selection procedure between EEC and ECS, the EEC should be pre-configured with or have discovered the address (e.g. URI) of the ECS as specified in clause 8.3.2 of TS 23.558[4]. The shared key-based authentication with certificate-based AF authentication or shared key-based mutual authentication using TLS between UE and AF as specified in Annex B of TS 33.535[2] or clause 5.3 and 5.4 of TS 33.222[3] is used for the authentication mechanism selection. In this case, EEC takes the role of UE and ECS takes the role of AF respectively.

6.9.3 Solution evaluation

This solution addresses KI#2.2 by authentication mechanism selection between EEC and ECS.

This solution based on TLS authentication protocols introduces no impact to network entities and existing procedures.

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

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