**3GPP TSG-SA3 Meeting #109 AdHoc-e Draft\_S3-230210-r1**

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

**Source: OPPO**

**Title:** **Address an EN in Sol #9**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***This pCR proposes to address an EN in Sol #9 of EDGE security***

# 2 References

[x] 3GPP TR 33.737

# 3 Rationale

This contribution proposes to resolve the following EN in Solution #9: Authentication mechanism selection procedure between EEC and ECS.

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

This EN can be addressed. The home network of the UE (EEC) may support one or multiple authentication mechanism (TLS with AKMA, TLS with GBA, or other TLS authentication methods), and there is a list for authentication mechanism supported by HPLMN, which is ordered according to a priority decided by the operator. The edge enabled UE (EEC) obtains the HPLMN supported mechanism list during registration, and choose mechanism based on HPLMN supported mechanism list and its security capability.

However, it has been studying to support AKMA in roaming scenario, and the authentication negotiation between UE (EEC) and the VPLMN should be allied with the conclusion of the KI#1 of TR 33.737[x], which is FFS.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\* Begin 1st change\*\*\*\*\*\*\*\*\*

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, TLS authentication methods (e.g., TLS with AKMA as specified in TS 33.535 [2], TLS with GBA as specified in TS 33.222 [3], other TLS authentication methods that uses other than 3GPP subscription credential(s) which is out of 3GPP) should be used. 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 (e.g., TLS with AKMA [2], TLS with GBA [3], or other TLS authentication methods).

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]. There is a list for authentication mechanism supported by HPLMN, which is ordered according to a priority based on operator’s security policy. The EEC obtains the HPLMN supported mechanism list during registration, and chooses the authentication mechanism with highest priority based on HPLMN supported mechanism list and its security capability.

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.

This solution requires a method to provision an ordered list for authentication mechanism supported by HPLMN to the UE (EEC).

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.

\*\*\*\*\*\*\*\*\* End 1st change\*\*\*\*\*\*\*\*\*