**3GPP TSG-SA3 Meeting #109 AdHoc-e Draft\_S3-230214-r1**

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

**Source: OPPO**

**Title: Add an evaluation in Sol #11**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***This pCR proposes to add an evaluation in solution #11 of edge security***

# 2 References

[x] 3GPP TS 23.558

# 3 Rationale

This solution proposes to add evaluation for solution#11 of TR 33.739.

# 4 Detailed proposal

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

6.11.3 Solution evaluation

This solution addresses the security requirement of KI #2.2 i.e., selection of authentication mechanism for authentication procedures between EEC and ECS/EES.

This solution reuses the existing signalling and processes (i.e. EES registration and ECS service provisioning as specified in clause 8.4.4 and clause 8.3.3 of TS 23.558[x]) in ECS helping the authentication mechanism selection between EEC and EES. Specifically, The EES provides the supporting mechanism to the ECS during the EES registration. After receiving the authentication mechanism chosen by EEC and EEC’s security capability, the ECS can choose the authentication mechanism supported by EEC and EES, then provide the selection result as Edge configuration information to the EEC. Therefore, this solution can reduce signalling overhead comparing with separately negotiation method.

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

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.

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

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