**3GPP TSG-SA3 Meeting #107Adhoc-e *draft-S3-221377-r4***

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

**Source: OPPO, Apple**

**Title:** **New solution: Authentication mechanism selection in EDGE**

**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 TR 33.739 “Study on security enhancement of support for edge computing phase 2”.

[2] 3GPP TS 33.535 "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

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

 [4] 3GPP TS 23.558 “Architecture for enabling Edge Applications”.

3 Rationale

This solution addresses security requirement for authentication mechanism selection between EEC and ECS, EEC and EES of key issue #2.2 in TR 33.739[1].

4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.739[1].

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

6.X Solution #X: Authentication mechanism selection procedure between EEC and ECS

6.X.1 Solution overview

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

6.X.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]. 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.X.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.

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.

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

\*\*\*\*\*\*\*\*\*\*\* Second Change\*\*\*\*\*\*\*\*\*\*\*

6.Y Solution #Y: Authentication mechanism selection procedure between EEC and EES

6.X.1 Solution overview

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

6.X.2 Solution details

For authentication between EEC and EES, 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 EES, the EEC and the EES should be set 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 EES, the EEC should be configured with the address (e.g. URI) of the EES by the ECS as defined in clause 8.3.3 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 EES takes the role of AF respectively..

6.X.3 Solution evaluation

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

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

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 EES.

\*\*\*\*\*\*\*\*\*\*\*End of Second Change\*\*\*\*\*\*\*\*\*\*\*