**3GPP TSG-SA3 Meeting #103-e *S3-211711r1***

**e-meeting, 17- 28 May 2021**

**Source: Apple**

**Title: Evaluation on solution#17**

**Document for: Approval**

**Agenda Item: 5.8**

1 Decision/action requested

***It is proposed to add the evaluation in MEC TR 33.839.***

2 References

[1] 3GPP TS 23.558: "Architecture for enabling Edge Applications (EA)"

3 Rationale

This pCR proposes to add the evaluation on solution#17. ~~and also proposes to add one EN to the GPSI authentication part:~~

~~“Editor’s Note: when there are multiple GPSI and multiple EEC, it is FFS on the mapping relationshop between EEC IDs and GPSIs. ”~~

4 Detailed proposal

**\*\*\*\*START OF CHANGES \*\*\***

6.17 Solution #17: EEC/EES/ECS authentication and transport protection with TLS

6.17.1 Solution overview

This solution addresses the Key Issues

- KI#1 "Authentication and Authorization between EEC and EES",

- KI#2 "Authentication and Authorization between EEC and ECS",

- KI#3 "Authentication and Authorization between EES and ECS", and

- KI#6 "Transport security for the EDGE-1-9 interfaces".

It proposes

- To use TLS as specified in RFC 5246 [25] and RFC 8446 [19] for authentication and transport protection of the EDGE-1 (EEC-EES), EDGE-3 (EAS-EES), EDGE-4 (EEC-ECS), EDGE-6 (EES-ECS) and EDGE-9 (EES-EES) interfaces,

- To use token-based authentication as another solution option for the authentication of the EEC by the ECS and EES,

- To use an existing challenge-response protocol like e.g. HTTP Digest as specified in RFC 7616 [24] with AKMA pre-shared key for authentication of the GPSI used in communication between EEC and EES/ECS, and

- To use the IP address to GPSI translation API as another solution option for the authentication of the GPSI.

6.17.2 Solution details

6.17.2.1 Authentication and transport protection for the EDGE-1, EDGE-3, EDGE-4, EDGE-6 and EDGE-9 interfaces

This solution proposes to align the protection of the EDGE-1, EDGE-3, EDGE-4, EDGE-6 and EDGE-9 interfaces with similar mechanisms in existing 3GPP security specifications. It seems that especially the security mechanisms in TS 33.434 [23], i.e. the security mechanisms for SEAL, are applicable here. In TS 33.434 [23], the security mechanisms are different for the signalling control plane and for the application plane interfaces. For the signalling control plane, TS 33.434 [23] specifies that HTTPS shall be used, e.g. in clause 5.1.1.3 IM-UU:

"IM-UU reference point is used between the identity management client and the identity management server. The IM-UU between the Identity Management client and the Identity management server shall be protected using HTTPS as defined in [3], [4] and [5]. The profile for TLS implementation and usage shall follow the provisions given in 3GPP TS 33.310 [6], annex E."

EDGE-1, EDGE-3, EDGE-4, EDGE-6 and EDGE-9 are the interfaces between EEC, EES, ECS and EAS. They can be seen as control plane interfaces for the application traffic between Application Client and EAS. Hence it seems reasonable that the security mechanisms should align with the signalling control plane security mechanisms in TS 33.434 [23]. However, the application protocol for the EDGE interfaces is not yet determined. Although HTTP is common practice, it seems premature to specify the usage of HTTPS. Instead it is proposed to use TLS. If HTTP is chosen as application protocol, then this solution proposes to use HTTPS.

Summing up, the proposed security mechanism for EDGE-1, EDGE-3 EDGE-4, EDGE-6 and EDGE-9 is:

"EDGE-1, EDGE-3, EDGE-4, EDGE-6 and EDGE-9 shall be protected using TLS as specified in RFC 5246 [25] and RFC 8446 [19]. The profile for TLS implementation and usage shall follow the provisions given in 3GPP TS 33.310 [13], annex E."

Another solution for the authentication of the EEC by the ECS and EES is the usage of tokens instead of TLS certificate of the EEC. For this option, the following solution is proposed:

Solution for the interface EDGE-4: The authentication of the ECS and the transport security of the interface are realized by using TLS with server authentication using the server’s certificate issued by CAs in the PKI. For the first authentication of the EEC by the ECS, the token, including the EEC ID, provided by the ECSP of the EEC or by a trusted new entity (that could or could not be collocated with the ECSP) to the EEC is used. In the case of provision of token by the ECSP, it is assumed that there is a business relationship between the ECSPs of the EEC and ECS, ECSP of the EEC provisions an initial access token to the EEC, and the ECS can verify the token. After the authentication of the EEC, the ECS provides a token to the EEC in the initial access to be used for the next establishment of the communication between them. In the other accesses than the initial access, the ECS decides on whether a new access token is necessary or not, considering information such as the expiration time of the token.

Solution of the interface EDGE -1: The authentication of the EES and the transport security of the interface are realized by using TLS with server authentication using the server’s certificate issued by CAs in the PKI. For the authentication of the EEC by the EES, the EEC first gets a token from the ECS for this purpose and sends the token to the EES. It is assumed that there is a business relationship between the ECSPs of the ECS and EES and the EES can verify the token.

Editor's Note: Whether the token-based mechanism can be used to authenticate the EEC is FFS.

One comment on the identifiers used on these interfaces. TS 23.558 [2], clause 7.2, specifies different identifiers that could be relevant to this solution. For EDGE-1, EDGE-3, EDGE-4, EDGE-6 and EDGE-9, the identifiers EEC ID and EES ID look relevant. Hence this solution proposes to leave the identifiers for the TLS connection out of scope. This is also aligned with TS 33.434 [23] that does not specify which identifiers to use for HTTPS. Furthermore, authentication between applications on the UE (ACs) and servers (EASs) is often dependent on the Operating System of the UE, and thus not in scope of 3GPP.

Editor's Note: ID used for TLS connection is FFS.

6.17.2.2 Authentication of the GPSI in EEC-EES/ECS communication

TS 23.558 [2] specifies different interactions between EEC and EES/ECS that use the UE ID for identifying the UE. The UE ID is specified in clause 7.2.6 of TS 23.558 [2]. The only example for the UE ID is the GPSI.

The GPSI also requires authentication. This solution proposes to use AKMA for the generation of a shared key KECUEID = KAF between the UE and the EES/ECS, i.e. AKMA AF. The EEC and EES/ECS can then use the KECUEID for authentication of the GPSI.

In order to use the shared KECUEID for authentication of the GPSI towards the EES/ECS, a modern but simple existing challenge-response protocol seems most appropriate. If HTTP is used as application protocol, HTTP Digest as specified in RFC 7616 [24] would be a good candidate.

The identifier used for the KAF is the A-KID in AKMA where A-KID is a temporary identifier. To verify the GPSI the following steps are executed:

1. The EEC sends GPSI in addition to the A-KID to EES/ECS if the GPSI is available to the EEC. EES/ECS verifies the GPSI received from EEC with the one locally configured (if available).

2. The EES/ECS send the A-KID and an indicator requesting GPSI with the AF\_ID to the AAnF via NEF or directly depending on the location of EEC/ECS.

3. The AAnF fetches the GPSI from the UDM based on the SUPI which is part of AKMA context in the AAnF.

4.The AAnF checks whether the AF is authorized to get the GPSI. If the check is successful, the AAnF provides the KAF and the GPSI to the EES/ECS. Otherwise sends a related failure message.

Editor’s Note: How the AAnF checks the authorization of AF considering also multiple GPSI scenario is FFS. Whether user consent is sufficient and required is in the scope of user consent study.

~~Editor’s Note: when there are multiple GPSI and multiple EEC, it is FFS on the mapping relationshop between EEC IDs and GPSIs.~~

5. The EES/ECS checks whether the GPSI sent by the EEC and the GPSI received from the AAnF are same or not. If the check is successful, the KAF (KECUEID) is used for authentication as mentioned above.

Another solution option to authenticate the GPSI is the usage of IP address to GPSI translation API.

6.17.3 Solution evaluation

The solution requires updates to the AKMA technical specification TS 33.535.

The authentication of GPSI requires EEC/EES to support AKMA

**\*\*\*\*END OF CHANGES \*\*\***