**3GPP TSG-SA3 Meeting #102bis-e *S3-211036r1***

**e-meeting, 1- 5 March 2021**

**Source: Apple**

**Title: New solution for key issue#10**

**Document for: Approval**

**Agenda Item: 2.8**

1 Decision/action requested

***It is proposed to add a new solution in MEC TR 33.839.***

2 References

[1] 3GPP TR 23.748: "Study on enhancement of support for Edge Computing in 5G Core network (5GC)"

3 Rationale

This pCR proposes a new solution to address key issue #10.

4 Detailed proposal

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

6.X Solution #X: Authorization/authentication for discovery of new EAS during Edge Data Network change

6.X.1 Introduction

This solution addresses the security requirement for authentication/authorization during Edge Data Network change in the key issue #10.

SA2 already concluded that Solution #32 is the basis of the normative work, in which the SMF may provide EAS rediscovery indication and its optional associated impact field within NAS message to UE in the session break out case. The SMF makes the decision based on information provided by AF or based on SMF's local configuration. The impacted field includes information DNS Suffix (i.e. domain name), FQDNs or IP address ranges of the local DN, which is used to identify the impacted DNS records.

When UE discovers the new EAS, the authentication may be required again. This solution addresses the issue that how to decide on whether the authentication should be triggered again for the connection to new EAS.

This solution is based on the solution#32 in SA2 TR 23.748.

6.X.2 Solution details



Fig 6.x.2-1 CN instructed UE DNS cache flush

Step 1. The UE connected to the application server located in an edge computing network accessed via ULCL1. So the original data path from UE to application server is via ULCL1. When the UE moves, and SMF sees that the path using ULCL1 is no optimized, it decides that a new PSA (PSA2) is needed. It may already at this stage insert a new ULCL (ULCL2) and may keep or remove old ULCL1.

Step 2. SA2 defines that SMF sends DNS re-resolution indication to UE via PDU Session Modification Command. The DNS re-resolution indication may be associated with an area information, which is indicated by the IP segment, subnet info, a list of FQDNs or DNS suffixes. So that the UE knows which application the indication is about. Besides the DNS re-resolution indication, SMF shall also include the “authorization/authentication policy IE” in the PDU Session Modification Command to indicate whether the new authorization/authentication procedure is needed.

Step 3. The UE either remove or replace (i.e. with the new DNS record) the DNS records stored locally. If the area information is included in the DNS re-resolution indication, the UE only remove or replace the DNS records corresponding to that area information.

Step 3.1. UE decision: UE shall decide whether to initiate the authorization/authentication procedure according to the “authorization/authentication policy IE”. If the “authorization/authentication policy IE” indicates the authentication procedure is not needed, then UE should continue to perform the step 4 without authorization/authentication procedure, Or UE may not continue performing the step4 at all, which depends on the UE’s policy. If the “authorization/authentication policy IE” indicates the authorization/authentication procedure is needed, UE should perform the step 4 including the authorization/authentication procedure.

Step 4. The UE discovers a new EAS using ULCL. If ULCL was not inserted in step 1, a new ULCL will be inserted according to KI#1.

The UE connects to the new application server located in the edge computing network corresponding ULCL2.

 Editor’s Note: It is FFS whether UE needs to initiate the authentication used in the subsequent discovering procedures.

6.X.3 Solution Evaluation

TBD

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