**3GPP TSG-SA3 Meeting #101-e *S3-202897***

**e-meeting, 9 -20 November 2020** Revision of S3-20xxxx

**Source: CATT**

**Title: Update key issue #1 in TR 33.839**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***It is proposed to update KI#1. SA3 is kindly requested to approve this contribution.***

# 2 References

[1] 3GPP TR 33.839, v0.2.0

[2] 3GPP TS 23.558, v1.1.0

[3] 3GPP TS 23.501, v16.6.0

[4] 3GPP TS 23.003,v16.4.0

# 3 Rationale

The UE ID binding verification requirement was identified and agreed in the last meeting. This contribution proposes to add the requirement to Key issue #1.

# 4 Detailed proposal

\*\*\*\*\*\* FIRST OF CHANGE \*\*\*\*\*\*\*\*\*

## 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.558: "Architecture for enabling Edge Applications."

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

[4] 3GPP TR 23.758: "Study on application architecture for enabling Edge Applications".

[5] 3GPP TS 23.502: "Procedure for the 5G System; Stage 2".

[6] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[9] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[10] 3GPP TS 33.501: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[11] 3GPP TS 33.187: "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[12] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[13] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[x] 3GPP TS 23.501: "System Architecture for the 5G System".

[y] 3GPP TS 23.003: "Numbering, addressing and identification".

\*\*\*\*\*\* SECOND OF CHANGE \*\*\*\*\*\*\*\*\*

## 5.1 Key issue #1: Authentication and Authorization between EEC and EES

### 5.1.1 Key Issue Details

As per TS 23.558 [2], EDGE-1 reference point enables interactions between the Edge Enabler Server and the Edge Enabler Client. EDGE-1 reference point supports registration and de-registration of the Edge Enabler Client to the Edge Enabler Server, retrieval and provisioning of Edge Application Server configuration information; and discovery of Edge Application Servers available in the Edge Data Network.

Edge Enabler server provides functionalities to Edge Enabler client over EDGE-1 reference point such as provisioning of configuration information to Edge enabler client and support the functionalities of application context transfer.

Edge Enabler Client performs the functionalities like configuration information retrieval from the edge enabler server and discovering of the edge application servers available in Edge Data Network. The Edge Data Network is a local Data Network. Edge Application Server(s) and the Edge Enabler Server are contained within the EDN.

The UE is initially provisioned with the configurations required to connect to the Edge Data Network. Upon initial provisioning, the Edge Enabler Client of the UE registers with the selected Edge Enabler Server(s) from the list of provisioned Edge Enabler Server(s). Edge Enabler Client consumes service offered by the Edge Enabler Server, e.g. discovering Edge Application Servers in an area of interest. The procedure enables initialization or update of the Edge Enabler Client context information at the Edge Enabler Server. The Edge Enabler Client sends Edge Enabler Client registration request to the Edge Enabler Server. Edge Application Server discovery enables Edge Enabler Clients to obtain information about available Edge Application Servers of interest. The identification of the Edge Application Servers is based on matching query filters or Application Client Profiles provided in the request.

GPSI can be used as UE identifier inside and outside of 5G networks. as specified in TS 23.501[x] and TS 23.003[y]. As specified in TS 23.558[2], a new edge enabler layer is defined. In order to identify the UE's Edge Enabler Client, the UE uses Edge Enabler client ID as the client identifier at the edge enabler layer. And the Edge Enabler client ID may be used along with GPSI. Then the EEC uses two different identifiers towards the EES, EEC ID and UE identifier (could be GPSI)). Solutions to this key issue need to clearly state which identifier of the EEC they authenticate.

Editor's Note: It is FFS whether the EEC ID will be unique across different UEs.

Editor’s Note: Whether the binding issue between EEC ID and UE identifier is required is FFS.

### 5.1.2 Security Threats

When Registration, Discovery , Deregistration is used without authorization, malicious Edge enabler client receive a list of Services and topology structure within Edge Data Network from Edge Enabler Server discovery response message. Received information can reveal Edge Data Network’s topology (e.g. URI, IP address, number of Edge Application Servers, Application Server Functionalities, API type, protocols). Malicious Edge Enabler Client may use this information to launch attacks on Edge Data Network or use this information for competitive reasons.

### 5.1.3 Potential Security Requirements

Edge Enabler Server shall be able to provide mutual authentication with Edge Enabler Client over EDGE-1 Interface.

Edge Enabler Server shall be able to determine whether Edge Enabling client is authorized to access Edge Enabling Server’s services.

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