**3GPP TSG-SA WG6 Meeting #39-bis-e S6-201xxx**

**e-meeting, 12th – 20th October 2020 (revision of S6-201886)**

**Source: Tencent, InterDigital**

**Title: Pseudo-CR on key issue x: UAS Identification usage in application layer architecture**

**Spec: 3GPP TR 23.755**

**Agenda item: 8.5**

**Document for: Approval**

**Contact: shuaiizhao@tencent.com**

**1. Introduction**

A UAS may connect to a USS/UTM using a 3GPP network, wifi, internet, or other means of networking approach. Whichever way the connection happens, a USS/UTM may only use one identifier for communicating with the UAS. In North America, the FAA has nearly adopted ASTM [19]’s remote ID proposal. The current IETF DRIP WG [18] is making great progress to make such a UAS remote ID feasible in either a wireless or wireless network environment. In 3GPP’s perspective, such RID is called a CAA-level UAV ID.

Based on TR 23.754 architecture’s assumption:

* “A UAV can be replaced by another from a UAS.”
* “A UAV Controller can be removed from a UAS and replaced with another UAV Controller or a TPAE.”
* “The USS/UTM accesses 3GPP services (e.g. location services) for a UAV corresponding to the CAA-level UAV Identity by using the 3GPP UAV Identity (i.e. the GPSI).”

Two IDs may be associated with one UAS, namely a CAA-Level ID (ex: IETF DRIP RID) and 3GPP UAV ID (ex GPSI). Each id may be used separately or as a combination for the UAS tracking and management purpose, depending on the presence of each ID.

The current SA6 UAS architecture enables direct communication between the UAS application layer and USS/UTM using SEAL [9]. Once a 3GPP network connection has been successfully made, the subsequent communication between the UAS application layer and USS/UTM may solely rely on the ID(s) assigned either by the 3GPP network or a USS/UTM or a combination of both. Regulations regarding the usage of CAA-level UAV ID may be found in the FAA [17] and [18].

Therefore, there is a need to work on ~~UAS ID~~ UAV ID management within the UAS application layer based on the situations mentioned in SA2’s architecture assumption.

Editor’s notes: the assignment of either CAA-Level ID or 3GPP UAV ID is outside of SA6’s scope.

**2. Reason for Change**

New KI

**3. Conclusions**

This proposal identifies a new KI relating to UAS ID(s) usage in application layer architecture.

**4. Proposal**

It is proposed to agree on the following changes to 3GPP TR 23.755

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

## 5.x Key issue #X: UAS Identification usage in application layer architecture

Once a 3GPP network connection has been successfully made, the subsequent communication between the UAS application layer and USS/UTM may solely rely on the ID(s) assigned either by the 3GPP network or a USS/UTM or a combination of both. Base on TR 23.754 architecture’s assumption, components of a UAS may be changed/updated. Therefore, a UAV ID may also be updated along the process.

The current SA6 UAS architecture enables direct communication between the UAS and USS/UTM using SEAL [9]. Therefore, SEAL may need to be able to support the UAV ID(s) update to provide a seamless service to the UAS application layer.

Editor’s notes 1: the assignment of either CAA-Level ID or 3GPP UAV ID is outside of SA6’s scope.

Editor’s notes 2: the privacy aspect related to the usage of UAV ID(s) is out of scope of SA6

Hence, it is required to study the following:

* Whether and how SEAL can support dynamic UAV ID(s) update.
* Whether and how SEAL can be enhanced to support communication between UAS and USS/UTM using either ID or a combination of both.