1 BACKGROUND

TIA Subcommittee TR-45.2 has identified the need for a serving network (SN) to confirm that a successful *Authentication and Key Agreement* (*AKA*) has been completed by the SN for a specific subscriber. The SN would report the successful establishment of the new Security Association to the home network (i.e., HLR) when a subscriber first appears in the serving system.

This capability would always provide the HLR with an indication of the success of *AKA* by the SN. In conjunction with an indication from the SN of an *AKA* failure, the HLR would always receive a report of the outcome of AKA, even if an event (e.g., MS power-down prior to completion of *AKA* in a new SN) interrupted normal processing of the intersystem operations required for roaming.

This capability would prevent potential denial of service attacks in environments where a subscriber can roam into both:

a. 3GPP systems using *AKA*,

b. Other systems that do not implement authentication.

One set of potential attacks is based on the limitations of an Interworking Function (IWF) needed for interworking between GSM-based systems and *ANS-41* systems. These limitations are due to specific implementation aspects of the IWF (e.g., the unique identity of the VLR is not provided to the HLR) and to the inherent differences in the intersystem operations of the two types of networks.

2 POTENTIAL ATTACKS

One set of potential denial of service attacks require the coordinated efforts of two parties. (Such attacks have already been observed by wireless service providers.). One fraudulent user appears in a new 3GPP system. The SN (SN-1) requests Authentication data (*Authentication data request*) from the HLR. The Authentication data request is sent to an Interworking function (IWF). The IWF sends an *ANS-41* query to the HLR requesting authentication vectors. The home network responds with Authentication data. The mobile station is turned off and the SN abandons the processing for the mobile station with no further information flows toward the HLR.

A second mobile station then appears in a different SN (SN-2) that does not support authentication, and a registration request is initiated toward the HLR. The IWF sends a registration notification to the HLR. The HLR may not be able to determine that the registration notification has originated from a different SN (SN-2). The mobile station will then be registered in SN-2, and if there is an indication that the subscriber's UIM was inserted in a new terminal, the real subscriber will be denied service.