3GPP TSG SA WG3 Security — S3#36 **S3-040493**

23 - 26 November 2004

Shenzhen, China

Title:	**Control of simultaneous session in WLAN 3GPP IP access (scenario 3)**
Source:	**Ericsson, Siemens**
Document for:	**Discussion and decision**
Agenda Item:	**6.10**
Work Item:	**WLAN-IW**

1 Introduction

In the last SA3#35 meeting, Ericsson presented a set of discussion papers (S3-040747, S3-040748, S3-040749, S3-040750) showing the unfeasibility of having the same mechanism to control sessions in WLAN direct IP access (scenario 2) and in WLAN 3GPP IP access (scenario 3). The discussion paper had no objections from technical point of view, but it was commented that an alternative solution should be provided in order to have this feature for release 6. This discussion paper sketches a potential solution.

2 Discussion

WLAN 3GPP IP access (formerly called scenario 3) makes the access to 3GPP operator services possible for the user. The way to achieve this is to have a border node in the 3GPP network that acts as entry point from outside networks where the user has got IP connectivity. The user establishes a UE-initiated tunnel with the PDG in order to have a secure connection. Then the PDG will redirect the traffic to the proper system where the service is invoked in the 3GPP network.

The goal of the simultaneous session control in scenario 3 is to be able to restrict (in the 3GPP home network) the connections that a certain user can have simultaneously at a certain moment. This will help to prevent potential fraud situations, for example that a user is giving access to his/her (U)SIM to several devices. These devices access the (U)SIM to get security credentials and authenticate successfully to the 3GPP home network. Thereby, with only one subscription, an unlimited number of people get access to the 3GPP network.

The proposed mechanism to have this control in the 3GPP home network is to limit the number of W-APNs and IKEv2 security associations per W-APN that can be active at the same time. According to the current IKEv2 specifications (already approved by IESG, current status is *proposed standard*) and the latest CRs in 3GPP regarding this issue (see the approved CR S3-040751, Sending of W-APN identification), the activation of a W-APN implies the creation of a new IKE Security Association. Then, the 3GPP home network has to detect and limit the number of attempts of IKE Security Associations.

The IKE SA procedure in IKEv2 is authenticated with EAP SIM/AKA (IKEv2 allows to delegate authentication tasks to EAP based protocols). This means that the 3GPP AAA server has to be contacted for every new IKE SA establishment attempt. When a new W-APN is about to be activated, the AAA server will receive an EAP authentication indication, and shall proceed checking the *W-APN active flag*, as follows: If

the W-APN to be setup is already active, the authentication attempt will be rejected. The AAA server will have to maintain an “active yes/no” flag for every subscribed W-APN. This limits the IKE SAs per W-APN to one.

3 Conclusions

The presented solution eliminates the possibility of having two or more IKE SAs, for the same W-APN, active at the same time. No situation could be identified in which more than one IKE SA is needed for a W-APN to work. Furthermore, no additional security is obtained by using more than one IKE SA per W-APN. In this way, certain fraud situations where two or more devices with different IP addresses have simultaneous access to the same W-APN can be prevented.

Together with this discussion paper we propose a CR, and suggest to send LSs to the proper groups were potential changes are needed (SA2, CN1).