3GPP TSG SA WG3 Security — S3#31 **S3-030789**
18 - 21 November 2003
Munich, Germany

Title: **Draft Reply LS on Tunnel Establishment and Security Association**
Response to: **S3-030676** (S2-033813)
Release: **Rel-6**
Work Item: 3GPP-WLAN interworking

Source: **SA3**
To: **SA2**
CC: **-**

Contact Person:
Name: Anand Palanigounder
Tel. Number: +1 972-684-4772
E-mail Address: anand@nortelnetworks.com

Attachments: **S3-030741?**

Overall Description:

SA3 thanks SA2 for their LS on Tunnel Establishment and Security Association. SA3 has discussed the proposed architecture of introducing the concept of W-APN Resolution Gateway and concluded the following:

Regarding the assumption that it is possible to separate the IPsec tunnel establishment and tunnel data handling into separate nodes, SA3 concluded that currently no standard way of securely separating the IPsec tunnel establishment procedure (i.e. IKE) from IPsec tunnel data traffic is available. Also, there is currently no standard mechanism available to suitably adapt and transfer the IPsec security associations agreed during the tunnel establishment procedure from the R-GW to the Packet Data Gateway (PDG). Furthermore, a new protocol has to be developed in order to accomplish this. The informational RFC3053 on IPv6 tunnel broker was mentioned in the discussion, but it was recognised that this RFC was only a framework document, not providing a sufficient basis for the 3GPP work. Further, it was also noted by SA3 that interfaces from R-GW to WAG and from R-GW to PDG may need to be enhanced to inform them of the new or changed firewall or security policies.

On the question of whether there are any security advantages offered by protecting the PDG before user authentication/authorisation:

- SA3 re-iterates the conclusion of SA3's response to SA2's previous liaison on PDG addresses (S3-030475). Specifically, "SA3 believes that hiding the IP address of the PDG on GRX using NAT or other techniques would not be useful from a security point of view." (the IP address of the PDG could be hidden for non-authorized users, but after authentication and authorization, any user (including a non-authorised user who is passed the IP address) could initiate an attack to the PDG or to the R-GW).
- Even if a new mechanism is developed to separate the tunnel establishment authentication/authorisation point from tunnel termination point, security measures such as mitigation of DoS attacks (as communicated in an earlier LS to SA2 from SA3, cf., S3-030477) has to be now implemented at the WAG for the W-APN Resolution Gateway and possibly for the PDG as well.

Assuming that a W-APN Resolution Gateway serves more than one PDG, any attack on the Resolution Gateway will result in single point of failure for any further tunnel establishment requests, although the previously established tunnel(s) can continue. Still these previously established tunnels could be lost if any authorized user executes an attack to the PDG, and security measures are needed in the PDG to mitigate the effects of those attacks.

Based on the above considerations, SA3 concludes that the proposal to physically separate the RGW and PDG has at most only marginal security advantages. SA3 further concludes that these advantages are not commensurate with the additional cost and complexity introduced. In particular, SA3 is concerned about the lack of available solutions for a separation of tunnel establishment protocol endpoint and tunnel endpoint.

As a result, a model in which users obtain a PDG address through DNS and establish a tunnel with this PDG using standard procedures is acceptable to SA3 from a security perspective.

Actions:

To SA2:

SA2 is kindly asked to take the above conclusions from SA3 into account in selecting a suitable tunneling architecture.

Date of Next SA3 Meetings:

SA3#32	9 - 13 February 2004	Edinburgh, U.K. (TBC)
SA3#33	11 - 14 May 2004 (TBC)	Beijing, China
SA3#34	6 - 9 July 2004 (TBC)	USA