3GPP TSG SA WG3 Security — S3#34 **S3-040605**
July 6 - 9, 2004
Acapulco, Mexico

Title: LS on IPsec tunnels and W-APNs
Release: Rel-6
Work Item: WLAN

Source: SA3
To: SA2
Cc: -

Contact Person:
Name: David Mariblanca
Tel. Number: +34 913393422
E-mail Address: david.mariblanca@ericsson.com

Attachments: -

---

1. Overall Description:

SA3 has made an analysis about the use of single or multiple IPsec tunnels per W-APN.
The reason for this analysis is that, as SA2 has stated, the user can use more than one W-APN simultaneously. As the W-APN activation implies the setup of an IPsec tunnel between the WLAN UE and the PDG, it is not clear if the same IPsec tunnel should be used for all W-APNs, or if separate IPsec tunnels should be established for each W-APN.
SA3 has considered the following pros and cons for both solutions:

Single IPsec tunnel

This option can be considered secure enough, as IKEV2/IPsec provides the means to negotiate a wide range of security mechanisms (encryption, confidentiality, etc). Even if the W-APN which initiated the tunnel didn't have strong security requirements, if a more security-sensitive W-APN is activated the IPsec tunnel can be rekeyed and security associations re-negotiated.

Pros:
- Simple and easy to implement, in WLAN UE and PDG side. The IKE/IPsec connection has to be initiated only once. There is no need to initiate/finish the IKE/IPsec connections when the W-APNs are activated/deactivated
- Performance. Specially from WLAN UE side, a single tunnel is more optimal than multiple tunnels.

Cons:
- Traffic separation is not possible if some W-APNs connect to the same PDG. This may happen for example if the user wants to use simultaneously W-APNs that make use of IP address spaces that may collide. This may happen, for example, with a W-APN accessing home network services and another W-APN accessing a corporate intranet.

Multiple IPsec tunnels

This is possible to achieve as IKEv2 allows the creation of subsequent tunnels with the CREATE_CHILD_SA exchange. In this case the IP traffic may correspond to any of the activated W-APNs, so Security Policy Databases (SPD) have to be maintained in the WLAN UE and the PDG so that the IP packets are routed through their associated IPsec tunnel.

The pros of this option are:

- Customized security. Every W-APN can have a security level associated to it. For example, a W-APN accessing the internet through the home operator network may not need strong security mechanisms

(as the internet is not considered secure enough itself), while a W-APN accessing home network services may need to have encryption because the access to some services in the operator network may carry very sensitive data from a security point of view. Then a set of security requirements will be associated to every W-APN so that the IPsec tunnel is negotiated according to the W-APN needs.

- Allows traffic separation. W-APNs accessing networks with private IP address spaces can be routed separately to other W-APNs accessing public IP addresses, or even other private IP networks with which there may exist address collisions.

2. Conclusion:

The previous analysis shows that from security point of view both solutions are feasible and provide an acceptable level of security. Other aspects, included those mentioned here (performance, complexity) and those not considered by SA3 (e.g.QoS), should be assessed in order to take a proper decision.

3. Actions:

SA3 kindly asks SA2 to take into account the aspects considered above and the conclusion reached.

4. Date of Next TSG SA WG 3 Meetings:

TSG-SA3 Meeting #35	5-8 October 2004	Malta
TSG-SA3 Meeting #36	23-26 November 2004	Shenzhen, China