3GPP TSG SA WG3 Security — S3#34 **S3-040521**

6 - 9 July 2004

Acapulco, Mexico

Title: **IPsec tunnels and W-APNs**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **WLAN-IW**

1 Introduction

This discussion paper makes an analysis about the need of single or multiple IPsec ESP tunnels in scenario 3. Scenario 3, now called *WLAN 3GPP IP Access*, allows the user to access services in the 3GPP network through the WLAN access network. In order to start using a service, the user must activate a W-APN, which identifies the point of attachment and the network the user wishes to connect to.

As currently stated in TS 33.234, a secure IPsec tunnel must be established when a service is being used in scenario 3. This implies that the WLAN UE, upon activation of the first W-APN, must initiate the tunnel establishment with the 3GPP network node acting as the other end point of the tunnel, the Packet Data Gateway (PDG). Once the tunnel is established, the packets inside the IPsec tunnel will be decrypted by the PDG and sent to the network node implementing that service.

2 Discussion

The access to 3GPP services by means of a single W-APN seems to be easy: when the W-APN is activated the IPsec tunnel is established, and when the W-APN is deactivated, the IPsec tunnel is terminated. However, a user can have more than one W-APN in his/her profile, and according to TS 23.234, these W-APNs can be active simultaneously. It is not clear then what to do when a subsequent W-APN is activated.

A W-APN may correspond to a group of services which the operator, by having similar nature or behaviour, wants to control in a similar way. There may exist W-APNs like:

- internet.telefonica.com (to access internet through the 3GPP operator's network). Called W-APN A in this document
- services.telefonica.com (to access home operator services). Called W-APN B in this document

When a user wishes to use for example W-APN A, he/she will activate it and a tunnel setup will be initiated by the WLAN UE to the PDG, using IKEv2. When the tunnel is established, the WLAN UE starts sending and receiving packets to the PDG, which encrypts/decrypts them.

If now the user wants to activate W-APN B, there are two options: either the same tunnel is used to route and protect the traffic corresponding to W-APN B, or a new, separate tunnel is negotiated with the existing IKEv2 connection.

2.1 All W-APNs use the same IPsec tunnel

This option, as explained above, takes advantage of a previously initiated IPsec tunnel for subsequent W-APNs activation. The following advantages are identified in this option:

- Simple and easier 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

- Secure. If the IPsec tunnel is negotiated with an acceptable level of security, all services in all W-APNs will take advantage of such security. Even if the W-APN which initiated the tunnel didn't have strong security requirements (this could happen with W-APN A), if a more security-sensitive W-APN is activated (W-APN B) the IPsec tunnel can be rekeyed and SAs re-negotiated.

An important drawback of this option is:

- 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 W-APN B and W-APN A simultaneously. As the home operator network is an intranet with its own address space, the PDG will have to know it and be able to route all packets to the home operator network, instead of to the Internet (if other private networks are accessed, there may exist address collisions with public IP addresses and the IP addresses used by the home operator).

2.2 Separate IPsec tunnels for every W-APN

We can find these advantages in this approach:

- Customized security. Every W-APN can have a security level associated to it. For example, W-APN A could be reasonable to be used without encryption, as the access to Internet is not secure itself. However, W-APN B may need to have encryption because the access to some services in the operator network may carry very sensitive data from 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 (like W-APN B) can be can be routed separately to other W-APNs (like W-APN A) accessing public IP addresses. The problem of the address collisions is solved.

The disadvantages for this option are the advantages of the other one, that is:

- Worse performance of the WLAN UE. The WLAN UE may need to maintain simultaneously several security associations, and be able to distinguish the traffic to treat with these different security associations

- Complexity of the mechanism. The WLAN UE and the PDG have to be able to handle separate traffic for the different tunnels. The WLAN UE will have to know which traffic corresponds to each tunnel, and the PDG may need to configure virtual tunnels to where the services are terminated (for example to a VPN gateway if the W-APN is for corporate access)

IKEv2 allows creating subsequent tunnels with the CREATE_CHILD_SA exchange. As in this case the IP traffic may correspond to any of the activated W-APNs, 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.

3 Conclusions

The previous analysis shows that from security point of view both solutions are feasible. The other aspects mentioned here (performance, complexity) should be studied more in detail in order to take a proper decision. It is recommended that other groups are contacted in order to asses these aspects. An LS is suggested to be sent to SA2, together with this document.