06 - 10 October 2003

Povoa de Varzim, Portugal

Title:	**UE-Initiated Tunneling with IKEv2**
Source:	**Nokia**
Agenda item:	**7.10**
Document for:	**Discussion**

---

1 Introduction

SA#21 did not approve WLAN-IW stage 2 [1] due to concerns raised about end-to-end tunneling selected for scenario 3. However, the end-to-end tunneling was taken as a working assumption but to validate it, some concerns need to be addressed by SA2.

This contribution discusses the role of UE-initiated tunneling and proposes IPsec tunnel mode with IKEv2 [2] as a one potential solution.

2 Discussion

The goal is to avoid operator specific VPN solutions when choosing the protocol for end-to-end tunneling. Furthermore, the protocol details should be specified up to stage 3 in 3GPP to enable interoperability in a multi-vendor environment.

According to the SA2's decision the other end of the end-to-end tunnel is PDG (Packet Data Gateway), which can exist also in VPLMN. Additionally the traffic can be routed through VPLMN or the Internet.

2.1 SA2 requirements

TS 23.234 v2.0.0 [1] Ch 5.7.2, states the following requirements for tunneling:

- Minimal requirements to the underlying IP connectivity network, i.e. WLAN UE initiated tunnelling and tunnel establishment signalling can be deployed on top of generic IP connectivity networks
- Minimal impacts to the WLAN
- Establishment of trusted relationships (e.g. mutual authentication for both tunnel end-points) shall be possible
- Tunnel IP configuration of the WLAN UE may be obtained from/through the remote tunnel endpoint
- Set up secure tunnels between WLAN UE and remote tunnel endpoint. Especially support encryption and integrity protection during tunnel establishment and while transporting user data packets, if enabled.
- Remote IP address (inner IP):
    - The transport of IPv4 packets shall be supported
    - The transport of IPv6 packets shall be supported (e.g. in order to support IPv6 services like IMS)
- Local IP address (outer IP):
    - Tunnel shall be able to support IPv4 and IPv6 transport addresses
    - Non-routable in the public internet (e.g. private) WLAN UE's local IP addresses shall be supported
- The protocol should be fully specified and 3GPP should define its usage to enable multi-vendor inter-operability.

using legacy authentication, i.e. username/password and W-APN (WLAN APN).
- IP network selection by user choice. This could be realized for example by selecting a different W-APN for each IP network. For instance, the W-APN could be resolved to a PDGW IP address using DNS by the UE, or the W-APN could be included as a parameter in signaling.
- IP address and other IP configuration from the remote IP network
- Encryption and integrity protection for both tunnel establishment and user data packets.
- Transport of IPv6 in order to support IMS even if the WLAN AN or other intermediate networks were IPv4-only.
- Based on available standards, protocol details agreeable in 3GPP.
- Be capable of traversing NAPT (Network Address and Port Translation) boxes as they seem to be the legacy of WLAN IPv4 AN.

Tunnel establishment signalling is still open in SA2. It needs to be agreed in SA2 whether the PGD IP address is resolved from the UE by DNS resolution or from the WAG with the previous UE-to-WAG signalling.

2.2 IPsec tunnel mode with IKEv2

IPsec tunnel mode with IKEv2 has the above-mentioned properties.

IPsec tunnel mode with IKEv2 shall be used with EAP/SIM or EAP/AKA or any authentication method carried by EAP. It is for further study how the keys for tunnel establishment are obtained. It should also be considered whether a fixed policy definition shall be specified for this 3GPP case. Internal addressing, other configuration information and NAT traversal shall be also specified.

IPSec NAPT traversal functionality has been incorporated into many NAPTs. On top of that, IETF is working on a generic solution using UDP tunneling, draft-ietf-ipsec-udp-encaps-06 [4]. Earlier versions of this draft has been already implemented in commercially available products.

2.3 L2TP/IPsec

Nokia proposed L2TP/IPsec with IKE [3] as a candidate for end-to-end tunneling in SA3#28 May meeting. At that point of time SA3 did see the proposal premature as SA2 WLAN adhoc had still not decided between the two tunneling options. In May Nokia saw L2TP over IPsec as a feasible candidate as it was the only protocol which was unambiguously specified in IETF concerning IP-address and DNS fetching from remote network. Now, IKEv2 draft specification [2] has progressed in IETF so it is seen as a better choice.

2.4 Status of IKEv2

All issues in draft-ietf-ipsec-ikev2 [2] are closed and the current version is –10. There has been ipsec working group last call during the summer and all findings are corrected. Final format and technical content of the draft has been verified, so next steps will be IESG evaluation and IETF wide last call. This includes considerations on last possible dependencies concerning the draft.

It should be also noted that if IKEv2 is chosen it has to be included into the IETF dependency list.

3 Conclusion and proposal

IPsec tunnel mode with IKEv2 solution is going to be based on standards and enable easy migration from current legacy VPN solutions if operators choose to support them even before R6 commercial availability.

SA#21 has decided that end-to-end tunneling is the working assumption for scenario 3 tunneling. It is proposed that SA3 studies IPsec with IKEv2 for a secure VPN solution for UE-initiated tunneling in 3GPP-WLAN interworking scenario 3 and takes under further investigation the related design details.

[1] 3GPP TS 23.234, “3GPP system to Wireless Local Area Network (WLAN) Interworking, System Description (Release 6)”

[2] IETF Internet-Draft, "Internet Key Exchange (IKEv2) Protocol” http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-10.txt

[3] S3-030236, Discussion paper on UE-Initiated Tunneling with L2TP/IPSec, Nokia, SA3#28

[4] IETF Internet-Draft, "UDP Encapsulation of IPsec Packets” http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-06.txt