3GPP TSG SA WG3 Security — S3#29 **S3-030476**
15 - 18 July 2003
San Francisco, USA

Title: Reply to LS S2-03279 (=S3-030427) Address discovery using public DNS for WLAN interworking

Work Items: WLAN Interworking

Source: 3GPP SA3
To: 3GPP SA2
Cc:

Contact Person:
Name: Colin Blanchard
Tel. Number: +44 1473 605353
E-mail Address: colin.blanchard@bt.com

Attachments: none

SA3 thanks SA2 for their LS on Address discovery using public DNS for WLAN interworking. SA2 had asked SA3 to answer the following questions

- Is allowing IP address of the WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

- Is allowing IP address of the PDG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

SA3 would like to respond as follows:

It was not clear to SA3 about what is meant by "public DNS" and in fact the following elements need to be considered separately:

1. **DNS Client**: The UE DNS Client's resolver will use a recursive name server for its queries. The Client can get the IP address for the recursive name server via static configuration or DHCP. The DHCP occurs after authentication to the WLAN and could be configured to provide the recursive name servers to use for WLAN/3G interworking. This would require the WLAN operator to configure the DHCP to support this.

2. **Recursive Name Servers:** The Recursive Name Server answers recursive queries from the UE's on the WLAN. It performs the necessary non-recursive queries to other name servers to get the correct Resource Records. The WLAN operator or 3G operator could operate the Recursive Name Servers. These DNS servers could probably be configured to answer queries for host names on the Internet and for

host names on the PLMN. These DNS servers would have to be secured of course. **SA3 have assumed that a "public" Recursive Name Server might be considered one that can resolve names on the Internet (i.e., uses Internet DNS for resolving names) and allows all authenticated WLAN clients to use it. The Recursive Name Server should be configured so that only users on the WLAN can query it (not accessible from the Internet) and should be controlled by the operators according to the roaming agreement.**

3. **Delegated Name Servers**: These DNS servers hold the Resource Records (e.g., A records) for the WAG and/or PDG. **SA3 have assumed that these will be managed and controlled by the operators of the WAG or PDG. SA3 weren't sure whether "public" DNS referred to name servers that are accessible to queries from the Internet or perhaps sit on the Internet DNS tree?** However, it is not clear to SA3 what DNS tree will the WAG & PDG names be placed in, Internet or an alternate. For example, would it use an ICANN-assigned TLD or a special TLD (e.g.,. gprs).

On the specific question asked by SA2 on "Is allowing IP address of the PDG/WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking" SA3 would like to make the following comments:

1. If the Internet DNS is to be used, then the Recursive Name Servers have to have access to the Internet in order to query the root servers and TLD servers. It is not necessary that the Recursive Name Servers be reachable from the Internet other than to receive replies to its queries (e.g., it should not answer queries from the Internet). The Delegated Name Servers need to be reachable from the Recursive Name Servers, but it is not then necessary that they are reachable from the Internet

2. Addresses used in the GRX should not be re-used on the Internet. However, this possibility should be considered. The Delegated Name Servers should be sure to resolve to the correct PDG addresses.

3. If DNS servers are used for determining IP addresses of WAG or PDG for tunnel establishment purposes, SA3 does not see any issues in satisfying the 3GPP security requirements, as the security threats against the DNS servers can be mitigated using existing mechanisms, as is already is the case with many current DNS server deployments. It is also recognized that more can be done to secure the DNS, such as deployment of TSIG and/or relevant aspects of DNSSEC

4. As well as protecting the DNS servers themselves, the communication between the UE and the DNS server has to be secure from modification by an attacker e.g. through the use of 802.11 security on the air interface and network security between the AP and the DNS server.

Finally, it should be noted that as an alternative it might be possible to deliver the IP address of the PDG or WAG to the UE using EAP-AKA authentication instead of using DNS. However, it is recognised that it is far from trivial to pass additional information in EAP and at the moment, SA3 see no way to provide such information in EAP-SIM or EAP-AKA. If EAP-SIM/AKA were extended to carry the Home PDG address, then this would work in any environment in which EAP-SIM or EAP-AKA would work. It should be noted that this will not hide the IP address of the tunnel endpoint, it will only make its discovery inconvenient.

Conclusion

Based on the assumptions and mechanisms described above, SA3 believes the DNS could be used for discovery of either WAG or PDG addresses by the UE.

Action on SA2:

To comment on the assumptions highlighted in bold above

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp
SA3#30	6 – 10 October 2003	Porto
SA3#31	18 – 21 November 2003	London