3GPP TSG SA WG3 Security — S3#33 **S3-040373**
10 - 14 May 2004
Beijing, China

3GPP TSG-SA WG2 meeting #39 **Tdoc S2-041665**
Shenzhen/China, 19th – 23rd April 2004

Title: **Reply to Liaison on Service Discovery of BSF and PKI portal**
Reply to: **S3-030188 (S2-041105)**
Work Item: **Support for Subscriber's Certificates**
Source: **SA2**
To: **SA3**
Cc: -

Contact Person:
Name: Mark Watson
Tel. Number: +44 1628 434456
E-mail Address: mwatson@nortelnetworks.com

Attachments: none

1. Overview

SA2 thanks SA3 for the opportunity to review the address discovery mechanisms for the PKI portal and Generic Bootstrapping Function within 33.221 and 33.220 respectively.

SA2 would like to make the following comments:

- The proposed changes refer to the use of DHCP for discovery of the BSF address. SA2 is not aware of a DHCP option which would be appropriate for this, unless SA3 has recently communicated with the IETF on this matter. Certainly, the IMS specification which is referenced by SA3's text does not describe any procedures which could be used for this purpose. SA2 did not understand why there should be any relationship between IMS and GBA.
- DHCP is generally used as part of establishment of IP connectivity, not afterwards.
- It is not usually necessary for terminals to be provided with the DHCP server address, since DHCP requests are sent to the local subnet broadcast address. SA2 therefore did not understand the need for the OMA "Provisioning Content" specification (reference [7] in 33.220) to be used to provide the DHCP address.
- SA3 refers at one point to the 'bootstrapping service'. SA2's understanding was that GBA was not a service as such but rather a generic mechanism that would be available to a variety of services for the purpose of authentication. One such service is Subscriber Certificates. It could be expected that the services which make use of GBA will each need to define a mechanism by which the UE is provided with the server (NAF) address. It would seem not unreasonable to suggest that the BSF address could be supplied in the same manner. It is not clear what a UE would do with the BSF address alone, since it is only ever used in conjunction with a service which requires authentication.
- SA3 might like to consider the option of defining a default domain name for the BSF server and PKI portal of each PLMN. For example: `auth.mnc123.mcc345.3gppnetwork.org` and `pki.mnc123.mcc345.3gppnetwork.org`. These domain names can be derived by the UE from the MNC and MCC within the user's IMSI and then resolved to IP addresses using DNS.

2. Action

SA2 requests that SA3 take account of the above comments within their specifications.

3. Future meetings

3GPPSA2#40	17 - 21 May 2004	Sophia Antipolis	FR
3GPPSA2#41	16 - 20 Aug 2004	Montreal	CA
3GPPSA2#42	11 - 15 Oct 2004	Sophia Antipolis	FR
3GPPSA2#43	15 - 19 Nov 2004	KOREA	KR