

3GPP TSG WG3 Security — S3#21
27 – 29 November, 2001
Sophia Antipolis, France

S3-010683

Source: TSG-SA WG3

To: 3GPP T2

Cc: CN5

Title: Response to LS T2-010905 (S3- 010571) on VASP MMS connectivity

Contact: Colin Blanchard
Email: colin.blanchard@bt.com
Tel: +44 1473 605353
Mobile: +44 7711 191835
Fax: +44 1473 623910

At their meeting in Sophia Antipolis 27- 29 November, TSG SA WG3 considered the above liaison statement from T2 on the architecture and suggested functionality for VASP (Value Added Service Provider) Connectivity to MMS. (MultiMedia Messaging Service)

SA3 would like to inform T2 that, at present, there are no plans to introduce end-to-end encryption of traffic between 3GPP terminals/clients and external applications at a VASP.

Concerning the OSA gateway and VASP, security functions are provided by the OSA framework functionality. This includes authentication, authorization, accounting and encryption between the OSA gateway and the VASP as a network operator specified option. Hence, it is recommended if OSA can provide the required functionality, then this should be the preferred choice from a security perspective. If this is proves not to be possible, then SA3 will be able to provide advice on the potential threats and security features required once more details of the Relay Server, MM7 API functions and protocol as agreed with CN5 can be provided.