3GPP TSG SA WG3 Security – S3#18 **S3-010205**

21-24 May, 2001

Phoenix USA

Source: **BT**

Title: **Authentication aspects in IM**

Document for: **Discussion and Decision**

Agenda Item: **9.3**

Introduction

At S3#17bis it was agreed that the working assumption would be that the hop-by-hop integrity protection of session establishment (INVITEs) and the option to authenticate the user during re-registrations and the ability of the Network to force re-registration, provide adequate protection for session establishment. The re-registration timer can be reset to a new value when forcing a re-registration.

It was agreed that a mechanism to force re-authentication is required, but that this need not necessarily be triggered by INVITE. It was reported that SIP does not provide a mechanism for network-triggered re-authentication, but some form of event-triggered re-registration would be desirable for operators, so that they only generate signalling traffic for this when, e.g., a chargeable event occurs (i.e., not while the UE is idle). Operators would also require flexibility in their triggering policies. It was agreed that SA WG3 should send a LS to SA WG1 to receive verification whether step-by-step integrity protection of INVITEs would cover operator requirements and that no further authentication would be needed.
It was generally agreed as a working assumption that hop-by-hop integrity protection would be enough.

The meeting agreed that any justified arguments against this assumption should be forwarded to SA WG3 meeting #18.

This paper aims to widen the discussion with additional aspects to be taken into account.

When to authenticate

While authentication at registration is obviously a clear requirement, the ability to be able to authenticate mobile users at any time needs to be fully considered. This would allow:

1. Operators to perform per-session set up (e.g. based on INVITE) authentication to enable them to be fully satisfied that the session requester (or receiver) is who they claim to be.
2. Operators to perform authentication during ongoing sessions to determine whom the parties involved are. This would ensure that in the case of

excessively lengthy (high cost/value) communications the end parties are still correct.

Operators need the confidence that for chargeable events (such as session requests) they can authenticate during the session set-up as well as during the ongoing session should enable operators to selectively authenticate the user as required; for example for ‘1 in n’ sessions.

Conclusion

Within 3G R99 the ability to authenticate at any time gives real operator flexibility, this same flexibility should be available within IM in the R5 timeframe.

Contact: Colin Blanchard
BTexact Technologies
MLB1 PP8
Adastral Park
Ipswich
IP5 5RE
Phone +44 1473 605353
Mobile +44 07711 191835
Fax +44 1473 623910
colin.blanchard@bt.com