3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010115**

13 September, 2001

Sophia Antipolis, France

Source: **Hutchison 3G UK**

Title: **Potential Importance of Bi-directional Protection Profiles**

Document for: **Discussion/Decision**

Agenda Item:

In S3z010085 Siemens suggest that bi-directional Protection Profiles would be a sensible option if they imply no loss in functionality. This contribution aims to show that unless all MAPsec is applied to all messages (even ones requiring no protection), bi-directional Protection Profiles are necessary.

Suppose the SAs between two Network elements have different Protection Profiles in each direction. More specifically if NEa sends a particular MAP operation to NEb it needs no protection, but if NEb sends the same MAP operation to NEa it requires integrity protection. This means that if NEa initiates a MAP operation to NEb, then the first message is not put in a MAP security tunnel. When NEb wants to reply, it wants to put integrity protection on the message but it cannot, as the MAP operation is not carried in a MAP security tunnel. The problem exists because the security of a MAP message cannot be decided independently of the other messages in a MAP operation.

Even bi-directional Protection Profiles do not completely eradicate this problem. Suppose that the Protection Profiles are changed when a pair of new SAs is negotiated. If a MAP dialogue is initiated with the old SA, but responded to with the new SA (as the old one has timed out for example) the above problem exists. This can only happens in a small time window and can probably be avoided by not using a SA to initiate a MAP dialogue within a few minutes of its expiry time (is this sensible?).

In conclusion, bi-directional Protection Profiles are necessary while it is permitted to send MAP operations outside a MAPsec tunnel.