3GPP TSG SA WG3 Security — S3#20 **S3-010492**

16 - 19 October, 2001

Sydney, Australia

Source: **Hutchison 3G UK**

Title: **Flexibility of MAP Protection Profiles**

Document for: Discussion / decision

Agenda Item: 7.1 MAPsec

1 Introduction

Without introducing proprietary protection profiles, the current MAPsec Protection Profiles provide a very inflexible level of security. While we appreciate that this was in part deliberate, we also recognise that this rigidity makes patching weaknesses in the currently defined profiles impossible without changes to the standard.

There are two scenarios in which security upgrades may be required:

1. A new operation is introduced to MAP which introduces new MAP functionality and new security vulnerabilities.
2. An attack is discovered which involves currently unprotected operations.

Both scenarios can be solved by either changes in the standard or use of a proprietary protection profile. Waiting for the standard change is not a viable alternative in scenario 2. Furthermore if an implementation does not allow proprietary protection profiles, it may not be solvable at all with the current implementation.

Our main concerns with the profiles are:

- For future-proofing, it must be allowable to protect new MAP messages or messages that have no currently defined protection. Without proprietary protection profiles, this is not possible until the standard is changed.
- There should be Protection Profiles that allow all the messages to be protected.
- The split between Protection Profile Identifiers (PPIs) reserved for future standards use and PPIs reserved for proprietary use is not defined.
- There is limited scope for proprietary protection groups. A unique PPI is needed for each new protection profile. This PPI must be available in both PLMNs, which negotiated the protection profile. It is conceivable that at least as many proprietary protection profiles as standardised profiles are needed. There are not enough protection group bits to allow this.

2 Proposed Solutions

Two features are proposed.

2.1 Provision for Proprietary Protection Profiles

The following mechanism is proposed to allow many proprietary protection profiles:

Reserve protection bit 15 to indicate “proprietary protection profile”. The remaining bits can be used to identify the required protection profile.

This allows for up to 2^{15} = 32768 proprietary profiles without interfering with the protection groups currently defined.

2.2 Catch-all Protection Groups

Two new “catch-all” protection groups are suggested.

- Protection group 14: Apply encryption and integrity protection to everything (all non-error messages).
- Protection group 13: Apply integrity protection to everything (all non-error messages). It is envisaged that this group may be used in conjunction with other groups. Messages that require encryption will still be encrypted, while messages that would have been sent unprotected are integrity protected.

These catch-all groups allow for the blanket upgrading of MAP security. Applying one of these groups will be the simplest way of upgrading security, but at a cost of performance. Should the performance cost not be too great (now or in the future), then these are valuable profiles in their own right.

3 Decisions Sought

This contribution seeks two decisions.

Firstly, we ask S3 to agree to the principle of flexible MAP protection profiles and that the conditions outlined in Section 1 shall be met.

- It must be possible to increase the level of protection on messages independently of defining new standard protection groups.
- Proprietary protection profiles must be implemented.
- The split between standard and proprietary PPI.

Secondly, the solutions in Section 2 are proposed for inclusion in 33.200.