3GPP TSG SA WG3 Security — S3#16 **S3-000674**

Sophia Antipolis (France), 28th-30th November, 2000

Agenda Item: 10.7

Source: Ericsson

Title: Algorithm Selection for MAP Security

Document for: Discussion and Decission

1 Introduction

This contribution presents a preliminary analysis of the suitable algorithms to be used for MAP Application Layer Security.

A recommended list of encryption and MAC algorithms is also presented. The proposal recommends a mandatory algorithm (AES-Rijndael for encryption and SHA-1 for integrity/authenticity) and considers the support of other algorithms as an option (Twofish, MD5).

2 Background

Current specification of MAP application layer Security defines three main types of Protection Modes:

- Protection Mode 0: No Protection
- Protection Mode 1: Integrity/Authenticity
- Protection Mode 2: Confidentiality + Integrity/Authenticity

Integrity/Authenticity is achieved applying a Message Authentication Code (MAC) function and using the integrity key agreed during MAP-SA negotiation at Za interface.

Confidentiality is achieved applying an encryption algorithm and using the encryption key agreed during MAP-SA negotiation at Za interface.

The specific MAC and encryption functions suitable to be used for these purposes have not been yet specified. S3 should agree on a minimum set of algorithms to be supported in any implementation of MAP Security.

3 Candidate Algorithms

3.1 Encryption Algorithms

Encryption algorithm used for confidentiality protection of MAP Operations shall be built on symmetric block cipher functions.

On the other hand, it has been a guiding principle in the design of the 3G security architecture so far that all security algorithms used should be public, in order to enhance trust in the security of the overall system. This means that the proposed algorithms shall be published and IPR free. Algorithms such as IDEA, RC5, BEANO, … have not been considered in this contribution due to this reason.

Note: BEANO might be considered as a suitable Encryption algorithm once published and if the evaluation reports so recommends it.

As possible encryption algorithms candidates to be used for MAP Security we can find:

- **DES:** symmetric, secret key (56 bits), minimum information block (64bits). DES is not considered secure nowadays. DES is a very widely used symmetric encryption algorithm. DES is a block cipher with a 56-bit key and an 8-byte block size.
- **Triple DES:** based on DES algorithm, symmetric, secret key (112 or 168 bits, but from the security point of view the effective key length is less that this), minimum information block (64bits).
- **AES (Rijndael):** Rijndael is a block cipher with a variable block length (128, 192 or 256 bits) and key length (128, 192, or 256 bits). Both block length and key length can be extended very easily to multiples of 32 bits.
- **Blowfish:** Blowfish is a 64-bit block cipher with a variable-length key (32- to 448-bit key).
- **Twofish:** Twofish is a 128-bit block cipher with a variable-length key (128-, 192-, or 256-bit key). It has been one of the AES finalists.

In a first analysis, Rijndael can be considered as the most appropriate candidate algorithm to be used for confidentiality protection of MAP Operations. It has just been selected by the NIST (National Institute of Standards and Technology) as the Advance Encryption Standard meant to replace DES. For this reason, the support of DES and TripleDES should be discarded.

Other AES finalist like Twofish would be also recommendable, offering high reliability and being IPR free.

Blowfish, largely used nowadays, would be also recommendable although its performance is considered to be worse than Rijndael or Twofish.

3.2 MAC Algorithms

A Message Authentication Code is a hash computed from a message and some secret data. It is difficult to forge without knowing the secret data. Its purpose is to detect if the message has been altered.

Hash functions shall be used in order to convert the cleartext information within the MAP operation into a fixed-length hash. It is computationally hard to reverse the transformation or to find collisions.

As possible MAC Algorithms candidates to be used for MAP Security we can find:

- **SHA-1:** The Secure Hash Algorithm produces a 20-byte output. NIST and NSA designed it for use with the Digital Signature Standard and it is widely used nowadays.
- **MD5:** MD5 is a secure hashing function that converts an arbitrarily long data stream into a digest of fixed size (16 bytes).

Any of these hash functions are valid to provide authenticity/integrity protection to MAP Operations.

4 Recommendation

Similarly to the case of Kasumi as UEA/UIA, Ericsson proposes the mandatory support of one Encryption algorithm and one MAC algorithm for MAP Security. Then as an option, the support of other algorithms may also be provided.

The following table lists the algorithms recommended to be supported in MAP Security implementations:

Encryption Algorithms	MAC Algorithms
AES-Rijndael (Mandatory)	SHA-1 (Mandatory)
Twofish (Optional)	MD5 (Optional)
Blowfish (Optional)	