TSG-SA WG3 (Security) meeting #14
Oslo, 1st August – 4th August 2000

S3-000433

Agenda Item:

Source: Ericsson

Title: Security Association for MAP Security.

Document for: Discussion and decision

---

1 Introduction

Related work for MAP Security in R99 shows a three layered structure incorporating mechanisms for establishing secure signalling links between network nodes. In particular, Layer I is responsible for agreeing on a symmetric session key for each direction of communication between two networks X and Y based on asymmetric crypto system techniques.

S3 has lately identified that not only key information is enough in order to establish secure MAP communications at Layer III. A complete set of parameters that form the Security Association (SA) information between the two PLMNs must be transferred and even negotiated between the two co-operating networks at Layer I.

This contribution tries to agree on the concept of SA for MAP Security and also tries to define the relevant parameters that need to be transferred and negotiated.

2 Security Association for MAP Security

The security relation between two co-operating PLMNs is not only defined by the integrity/confidentiality keys that shall be used to secure their MAP communications. There are other number of parameters that also identify this Security Association (Algorithm identifiers and version numbers, Security policies and protection modes, SA lifetime …). It would even be advisable to allow for the negotiation of certain or all of these parameters on the course of the execution of Layer I mechanisms.

As an example for the need of transportation and negotiation of SA information other than Key information, just consider the following situations:

- In order to determine whether the protection mode (if any) indicated in a received MAP message is correct, the receiving entity must compare it against the applicable Security Policy. This Security Policy information might be pre-configured at each relevant NE in the receiving Network, but in order to provide a more flexible and automatic mechanism it shall be transferred from the sending entity in the course of execution of Layer I mechanisms.

- The Security Policy information transferred from sending to receiving entity might specify 'Secure Transport not required' for some ACs. In the event that the receiving entity is not willing to accept unsecure transport due to security considerations with the originating PLMN, it would be advisable that Layer I mechanisms allows for negotiation of this specific parameter. Negotiation would also be required for example in order to reach an agreement on specific algorithms to use, duration of the SA ….

As agreed in S3#13, contributions on MAP Security will be incorporated in a living document where MAP Security will be stabilised before it is introduced in R00 specifications. The following definition of Security Association for MAP Security is proposed to be included in that living document:

Security Association

A Security Association (SA) is a set of policy and key(s) used to protect information. The SA conveys information about the security parameters to be used for MAP message protection when MAP messages are to be sent from Network X to Network Y.

The agreement on a symmetric session key between two KACs for protection of their MAP message exchange is accomplished through the establishment of a SA.

A Security Association encompasses the following parameters:

- **Encryption Algorithm Identifier:**
  Identifies the encryption Algorithm used for MAP message protection.
- **Encryption Key Version Number:**
  Version number of the encryption key to be used for MAP message protection.
- **Encryption Key:**
  Encryption Key to be used for MAP message protection.
- **MAC Algorithm Identifier:**
  Identifies the MAC Algorithm used for MAP message protection.
- **MAC Key Version Number:**
  Version number of the MAC key to be used for MAP message protection.
- **MAC Key:**
  MAC Key to be used for MAP message protection.
- **Security Policy:**
  Indicates whether a MAP dialogue needs protection, and if so, indicates for every component of the dialogue the protection mode and mode of operation of the encryption algorithm to be used. In case protection is required, it shall be also stated whether fallback to unprotected mode is allowed.
- **SA Lifetime:**
  Defines the actual duration of the SA.

These parameters shall be transferred, in a secure manner, between the respective KACs of the co-operating networks in the course of execution of Layer I mechanisms.

The possibility to negotiate security attributes shall be provided to some extent, so that both communicating Networks may arrange the encryption/MAC algorithms and parameters, the security policy or even the SA lifetime.