3GPP TSG-SA3 Meeting #15bis
(Ad-hoc on aSIP and NDS WIs)
Munich, 8th – 9th October 2000

S3z000014

Agenda Item: -

Source: Ericsson

Title: Protection Profiles for MAP Security

Document for: Information and Discussion

1 Introduction

This contribution tries to agree on a definition for Protection Profiles for MAP Application Layer Security and on a criteria for its specification and selection.

A draft proposal for Basic MAP-PPs is also presented.

2 Background

S3 has progressed the work on MAP Application Layer Security as a WI for R00, especially on the field of Key Management (Z_A and Z_B interfaces, former Layers I and II). As a consequence, the use of Security Associations for MAP Security has been agreed. MAP SAs are used to define the security parameters required to protect the traffic over the Z_C interface (the SS7 network).

The agreement on a MAP-Protection Profile (MAP-PP) is part of the information required as part of the MAP- SA negotiation procedure.

3 Protection Profiles for MAP Security

3.1 Definition of MAP Protection Profile (MAP-PP)

3GPP TR 33.800 v0.2.4 ('Principles for Network Domain Security') includes the following definition of MAP-PP:

- ***MAP Protection Profile:***
  A MAP Protection Profile (MAP-PP), is an specification of how components in a MAP message over Z_C interface shall be protected. 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 also state whether fallback to unprotected mode is allowed.

As discussed in S3z000013 ('General Structure of Secure MAP Operations' also presented to this meeting), Ericsson's understanding is that S3 should be focused on the definition of protection mechanisms on a per-MAP Operation basis; i.e. define what MAP operations require protection and what kind of protection (confidentiality/integrity).

In addition, it is proposed to consider the indication of fallback to unprotected mode as a separate parameter within the MAP-SA since this shall apply to the complete set of MAP operations specified within the MAP-PP. This fall back option is mainly to allow stepwise deployment of MAPSec (some nodes are upgraded while others aren't), so either a node will be able to apply a MAP-PP or not at all.

It is also proposed to remove the mode of operation of the encryption algorithm from the definition of MAP-PP.

Therefore, Ericsson would like to modify the definition of MAP-PP to:

- ***MAP Protection Profile:***
  A MAP Protection Profile (MAP-PP), is an specification of how MAP operations over Z_C interface shall be protected. Indicates whether a MAP operation needs protection, and if so, indicates the protection mode to be used.
- ***Fallback to Unprotected Mode Indicator:***
  In case protection is required, this parameter indicates whether fallback to unprotected mode is allowed.

3.2 Criteria for defining MAP-PPs

The main goal of MAP Application Layer Security is to protect from eavesdropping and manipulation of Signalling data between two communicating MAP entities. This takes especial relevance in the event the MAP communicating entities belong to different network domains; i.e. two NEs (e.g. HLR and VLR) in different PLMNs communicating via MAP protocol over the public SS7 network.

Not all the information carried over the MAP Protocol can be considered as critical. As a first approach, the most sensitive data subject to be protected comprises:

- Authentication information (Authentication vectors, security context, etc …).
- Subscriber Identity information (IMSI, MSISDN).
- Subscriber Location information (MSC address, Location Area …).
- Subscriber Services information (Services subscribed to, allowed to use …)
- Charging information (CDRs).

Therefore, main criteria at the time of defining a MAP-PP would be to try to protect MAP operations which carry sensitive information (authentication, identity, location, services or charging information) between the Home and Visited Environment (e.g. HLR <--> VLR).

The following preliminary list of critical MAP operations carrying sensitive information can be made:

MAP Operation	Authentication Info	Location Info	Services Info
UpdateLocation		✓	
UpdateGprsLocation		✓	
PrepareHandover	✓		
ForwardAccessSignalling	✓		
SendIdentification	✓		
PrepareSubsequentHandover		✓	
SendAuthenticationInfo	✓		
InsertSubscriberData			✓
DeleteSubscriberData			✓
AnyTimeInterrogation		✓	
ProvideSubscriberInfo		✓	
AnyTimeSubscriptionInterrogation			✓
AnyTimeModification			✓
ProvideRoamingNumber		✓	
Register/erase/(de)activate/interrogateSS + register/getPassword + (process)UnstructureSS-Request/Notify			✓

NOTE1: Mind that most of the MAP operations include the IMSI as user identifier and that there is no MAP operation that carries charging information. This is why these factors have not been considered in the table.

NOTE2: MAP operations like “PrepareHandover”, “PrepareSubsequentHandover”, “ForwardAccessSignalling” and “SendIdentification” take place during Roaming and Handover procedures between two MSCs/VLRs. These MSCs/VLRs might belong to different network domains in the case of Intersystem Roaming/Handover, but Network Operators do not always allow these kind operations in this case. Besides, this kind of operations are not supposed to happen very often and the value to provide protection to them is then questioned.

MAP operations handling Authentication and/or Location information shall be protected with Protection Mode 2 (authenticity/integrity and confidentiality) and MAP operations handling Service information shall at least be protected using Protection Mode 1 (authenticity/integrity).

In addition, it shall be prevented that an attacker may simulate MAP operations like Reset, causing system malfunction. Such operations shall be protected using at least Protection Mode 1 (authenticity/integrity). However this kind operations have not been considered in this analysis.

3.3 Proposal of Basic MAP-PPs

Based on the above mentioned principles, one could make multiple combinations and create multiple MAP-PPs. Ericsson proposes the definition of the following basic MAP-PPs:

MAP-PP(0): Protection for Authentication Information

This MAP-PP will protect Authentication information. The MAP operations subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (authenticity/integrity and confidentiality)

The rest of MAP operations not included in this list are considered not to be protected (Protection Mode 0).

MAP-PP(1): Protection for Authentication and Location Information

This MAP-PP will protect Authentication and User Location information. The MAP operations subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (authenticity/integrity and confidentiality)
UpdateLocation	2 (authenticity/integrity and confidentiality)
UpdateGprsLocation	2 (authenticity/integrity and confidentiality)
AnyTimeInterrogation	2 (authenticity/integrity and confidentiality)
ProvideSubscriberInfo	2 (authenticity/integrity and confidentiality)
ProvideRoamingNumber	2 (authenticity/integrity and confidentiality)

The rest of MAP operations not included in this list are considered not to be protected (Protection Mode 0).

MAP-PP(2): Protection for Authentication, Location and Service Info

This MAP-PP will protect Authentication, User Location and Service information. The MAP operations subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (authenticity/integrity and confidentiality)
UpdateLocation	2 (authenticity/integrity and confidentiality)
UpdateGprsLocation	2 (authenticity/integrity and confidentiality)
AnyTimeInterrogation	2 (authenticity/integrity and confidentiality)
ProvideSubscriberInfo	2 (authenticity/integrity and confidentiality)
ProvideRoamingNumber	2 (authenticity/integrity and confidentiality)
InsertSubscriberData	1 (authenticity/integrity)
DeleteSubscriberData	1 (authenticity/integrity)
AnyTimeSubscriptionInterrogation	1 (authenticity/integrity)
AnyTimeModification	1 (authenticity/integrity)
Register/erase/(de)activate/interrogateSS + register/getPassword + (process)UnstructureSS-Request/Notify	1 (authenticity/integrity)

The rest of MAP operations not included in this list are considered not to be protected (Protection Mode 0).