3GPP TSG-SA3 Ad Hoc on 'Network Domain Security' **S3z010033**
Madrid 23-24 April, 2001

Some minor changes since yesterday are revision marked below.

Source:	**TSG-SA WG 3 ad hoc on network domain security**
Title:	**MAP security**
To:	**TSG-CN WG4**

Contact Person:

Name: Peter Howard

E-mail Address: peter.howard@vf.vodafone.co.uk

Tel. Number: +44 1635 676206

TSG-SA WG3 thank TSG-CN WG4 for their LS on MAPSec [N4-010176] and provide the following information on progress.

1 Introduction

Three topics are covered:

- MAP protection profiles
- Structure of security header
- Algorithm mode selection for MAP security

Additionally S3 ad hoc would like to inform N4 that the coding of MAP security elements should be contained as ASN.1 in TS 29.002 based on stage 2 specifications to be included in TS 33.200.

2 MAP protection profiles

2.1 Protection mode

There are three modes of protection which may be applied to a MAP payload:

- Protection mode 0: no protection
- Protection mode 1: integrity protection only
- Protection mode 2: integrity protection and ciphering

It is required to define MAP protection profiles which determine the protection mode that is applied to each MAP payload.

2.2 Granularity of protection

Three options for defining MAP protection profiles (MAP-PP) have been discussed in S3:

- MAP-PPs defined at MAP Application Context level
- MAP-PPs defined at MAP Operation level
- MAP-PPs defined at MAP Operation Component level

Pros and cons of each option have been discussed.

MAP-PPs per MAP-AC would be really easy to define and maintain but they would provide poor granularity (MAP dialogues with a little security interest will still be protected). Definition of MAP-PPs per MAP-AC was not considered as the preferred option due to its poor granularity.

MAP-PPs per MAP-Operation would be still easy to define and maintain while providing a good granularity.

MAP-PPs per MAP-Component would provide the most precise granularity. Since different components of the same dialogue could be protected with different protection modes (e.g. invoke=PM1, result=PM2, error=PM0) this would allow some saving in processing capacity.

It was agreed that there is no difference between an operation level definition and a component level definition from a security point of view.

S3 thinks that among the criteria to be considered for the decision on component level protection or operation level protection could be: processing capacity, administration effort, ease of implementation and integration into MAP processing.

S3’s current working assumption is that the processing saving is not a major issue and therefore assume an operation level definition. N4 are asked to voice their opinion on this assumption. **Unless N4 present technical arguments to change the S3 ad hoc view, the working assumption shall be endorsed at S3#18 (21-24 May 2001).**

2.3 Fallback to unprotected mode indicator

A “fallback to unprotected mode indicator” is required by a network element to allow stepwise deployment of MAPSec (some nodes are upgraded while others are not). This indicator is included as a separate item in the security association rather than integrated as part of the MAP protection profile. This is done to avoid the need to define two different protection profiles for the same set of operations, one allowing and the other not allowing fallback to unprotected mode.

2.4 MAP protection groups

Note: This section describes both the operation level and component level options. The protection groups defined in this section are still under consideration in S3.

The following groups of messages and their protection modes are defined at both the operation level and the component level. Protection profiles can then be individual protection groups or particular combinations of groups.

Combinations of overlapping protection groups are forbidden. Forbidden combinations are explicitly specified in 2.4.1 below.

The concept of "protection levels" is introduced to administrate the protection on component level: A protection level of an operation determines the protection modes used for the operation's components according to the following table:

protection level	protection mode for invoke component	protection mode for result component	protection mode for error component
1	1	0	0
2	1	1	0
3	1	2	0
4	2	1	0
5	2	2	0

2.4.1 MAP-PG examples

MAP-PG(0): No Protection

This MAP-PP does not contain any operation and it does not protect any information. It is useful however to have a "null" MAP-PP to use on situations where no security is required or is an option. This protection group cannot be combined with any other protection group.

MAP-PG(1): Protection for Reset

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
ResetContext-v2/ Reset	1	1
ResetContext-v1/ Reset	1	1

MAP-PG(2): Protection for Authentication Information except Handover Situations

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
InfoRetrievalContext-v3/ Send Authentication Info	2	3
InfoRetrievalContext-v2/ Send Authentication Info	2	3
InfoRetrievalContext-v1/ Send Parameters Not possible to make the protection dependant on the contents of the message	2	3
InterVlrInfoRetrievalContext-v3/ Send Identification	2	3
InterVlrInfoRetrievalContext-v2/ Send Identification	2	3

MAP-PG(3): Protection for Authentication Information in Handover Situations

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
handoverControlContext-v3/ Prepare Handover (Note that the AC contains also other operations)	2	4
handoverControlContext-v3/ Forward Access Signalling (Note that the AC contains also other operations)	2	TBD
handoverControlContext-v2/ Prepare Handover (Note that the AC contains also other operations)	2	4
handoverControlContext-v2/ Forward Access Signalling (Note that the AC contains also other operations)	2	TBD
handoverControlContext-v1/ Perform Handover (Note that the AC contains also other operations)	2	4
handoverControlContext-v1/ Forward Access Signalling (Note that the AC contains also other operations)	2	TBD

MAP-PG(4): Protection of Location Information

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
networkLocUpContext-v3/ Update Location (Note that the AC contains also other operations)	2	4
gprsLocationUpdateContext-v3/ Update GPRS Location (Note that the AC contains also other operations)	2	TBD (2 0 0)
handoverControlContext-v3/ Prepare Subsequent Handover (Note that the AC contains also other operations)	2	T B D (2 0 0)
subscriberInfoEnquiryContext-v3/ Provide Subscriber Info	2	3
networkLocUpContext-v2/ Update Location (Note that the AC contains also other operations)	2	4
handoverControlContext-v2/ Prepare Subsequent Handover (Note that the AC contains also other operations)	2	T B D (2 0 0)
networkLocUpContext-v1/ Update Location (Note that the AC contains also other operations)	2	4
handoverControlContext-v1/ Perform Subsequent Handover (Note that the AC contains also other operations)	2	T B D (2 0 0)

MAP-PG(5): Protection of AnyTimeModification requests (a)

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
AnyTimInfoHandlingContext-v3 / AnyTimeModification	1	1

This grouping cannot be combined with MAP-PG(6).

MAP-PG(6): Protection of AnyTimeModification requests (b)

Application Context/Operation	Protection Mode (Operation level)	Protection Level (Component level)
AnyTimInfoHandlingContext-v3 / AnyTimeModification	2	5

This grouping cannot be combined with MAP-PG(5).

2.5 Protection profiles

Note: This section describes both the operation level and component level options. The protection profiles defined in this section are still under consideration in S3.

Protection profiles can be individual protection groups or particular combinations of protection groups. MAP protection profiles are coded as a 16 bit binary number where each bit corresponds to a protection group. Currently only 7 groups are defined, the rest are reserved for future use.

Protection profile bit	Protection group
0	No protection
1	Reset
2	Authentication information except handover situations
3	Authentication information in handover situations
4	Location information
5	Anytime modification (a)
6	Anytime modification (b)
7-15	Reserved

The following examples of protection profiles can be defined:

Protection profile name	**Protection group**						
	No protection	**Reset**	**Authinfo except handover situations**	**Authinfo in handover situation**	**Location information**	**Anytime modification (a)**	**Anytime modification (b)**
Profile A	✓						
Profile B		✓	✓				
Profile C		✓	✓	✓			
Profile D		✓	✓	✓	✓		
Profile E		✓	✓	✓	✓	✓	
Profile F		✓	✓	✓	✓		✓

3 Structure of Security header

N4 Question:

- **Structure of Security Header**
  The attached CR 168r1 to 29.002 modifies the internal structure of the Security Header according to the SA3 agreements.
  Can SA3 please confirm that a single Initialisation Vector (IV) in the Security Header is sufficient, i.e. if in protection mode 2 both the encryption Algorithm and the Integrity/Authenticity Algorithm require an IV, the same IV will be used.

- The answer: One IV shall be included in the security header. It will have a length of 8 bytes.

4 Algorithm Mode Selection for MAP Security

N4 Questions:

- **Algorithm Selection for MAP Security**
  The selected Encryption Algorithm (AES) and the selected Integrity/Authenticity Algorithm (AES-MAC) may be used with various key lengths, block lengths and modes of operations. Furthermore the length of the Integrity Check Value produced by AES-MAC is not fixed. The length of the additional message overhead introduced by MAPSec very much depends on the chosen block length (IV length, padding), mode of operation (IV present/absent, padding present/absent) and on the length of the Integrity Check Value. Concerns have been raised that the additional overhead may result in an available message length for the MAP application which does not allow a single Authentication Quintet to be carried in worst case scenarios.
  SA3 are asked to refine their algorithm selection by determining

  - the block length which is to be mandatorily supported,

- Answer: AES block length to be mandatorily supported is 128 bits but the padding requirement depends on the mode of operation, see later answer for the question about encryption mode.

  - the key length which is to be mandatorily supported,

- Answer: the mandatorily supported length is 128 bits for both integrity and encryption key.

  - the mode of operation for AES which is to be mandatorily supported,

- Answer: The exact mode for AES (stream or block cipher mode) is still to be decided. Stream cipher mode implies that no padding is needed because of encryption, but its suitability requires further study.

  - the mode of operation for AES-MAC which is to be mandatorily supported,

- Answer: The working assumption is AES-CBC-MAC mode but the exact details are not available at the moment.

  - the length of the Integrity Check Value which is to be mandatorily supported
  in a way which minimises the overhead as far as possible while ensuring an acceptable level of security.

- Answer: The length should be 64 bits but S3 could agree on a smaller length (minimum 32 bits) in case this would give essential efficiency improvements (e.g. in the form of avoiding segmentations).