3GPP TSG-SA3 Meeting #15bis7 S3-z010057014
(Ad-hoc on aSIP and NDS WIs)
GöteborgMunich, Sweden, 278th – 9th FebruaryOctober- 2nd March 20010

Agenda Item: tbd (NDS WI)

Source: Ericsson

Title: Protection Profiles for MAP Security

Document for: Information and Discussion and Decision

1 Scope and Objectives

This contribution tries to agree on the definition for Protection Profiles for MAP Application Layer Security. A draft proposal for Basic MAP-PPs is also presented.

2 Background

SA3 has agreed on many issues related to securing MAP traffic on SS7 networks. The MAP Protection Profiles that are necessary to define which MAP operations are in fact secured have not been agreed yet. In order to get MAP security ready in Release 4 timeframe, SA3 needs to agree on the structure and content of MAP Protection Profiles. Especially members representing network operators are urged to voice their opinion on the level on which they wish to manage the network.

Three different alternatives for the level on which to define MAP Protection Profiles have been discussed in SA3:

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

It has been agreed that there is no difference between the alternatives from security point of view. The differences come from the complexity of implementation and management versus flexibility of applied security level and possible load optimisation.

At S3#16 meeting, SA3 concluded that MAP-PPs both at MAP-AC level and MAP-Operation level were sufficient. However, CN4 comments on this SA3 decision (refer to LS in Tdoc N4-010176) and asks SA3 to still consider definition of MAP-PPs at component level as a valid option.

This document will try to present the alternatives and discuss on the pros and cons for each one.

3 Protection Profiles for MAP Security

3.1 Fallback to Unprotected Mode Indicator

The “fallback to unprotected mode indicator” 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 anticipated that in the future when all the networks have been upgraded to fully support MAP security, the fallback indicators will loose their justification. For this reason the fallback to unprotected mode indication is proposed to be part of policy data and their

definition subject to operator agreements. It is be necessary to distribute the fallback indication from the KAC to NEs together with the SAs.

Moreover, the proposed handling of this indicator ease the further definition and administration of MAP-PPs (e.g. if the indication is included as part of the MAP-PP itself, there will be the need to define two different MAP-PPs for the same set of operations, one allowing and another not allowing fallback).

3.2 Proposal for Basic MAP-PPs

It is possible to make multiple combinations and create multiple MAP-PPs. It is proposed that a limited number of basic MAP-PPs is standardised in Rel 4. The MAP-PPs here are defined both against operations and components to help SA3 members to decide on their view on which is the best alternative for MAP-PP structure.

Proposal for basic MAP-PPs:

MAP-PP(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.

MAP-PP(1): Protection for Authentication Information

This MAP-PP will protect Authentication information in other than handover situations. The MAP dialogues identified by the application context and operations as well as their components within these dialogues subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:

Application Context/Operation	Protection Mode	Component	Protection Mode
infoRetrievalContext-v3/ Send Authentication Info	2	Invoke	1
		ReturnResult	2
		ReturnError	0
infoRetrievalContext-v2/ Send Authentication Info	2	Invoke	1
		ReturnResult	2
		ReturnError	0
infoRetrievalContext-v1/ Send Parameters (only if requested parameterList includes requestAuthenticationSet)	2	Invoke	1
		ReturnResult	2
		ReturnError	0
interVlrInfoRetrievalContext-v3/ Send Identification	2	Invoke	1
		ReturnResult	2
		ReturnError	0
interVlrInfoRetrievalContext-v2/ Send Identification	2	Invoke	1
		ReturnResult	2
		ReturnError	0

Additionally, MAP-PP(1) proposes the protection other critical MAP dialogues such us:

Application Context/Operation	Protection Mode	Component	Protection Mode
resetContext-v2/ Reset	1	Invoke	1
resetContext-v1/ Reset	1	Invoke	1

The rest of MAP dialogues identified by Application Contexts not included in this list are considered not to be protected. Also other operations within the listed Application Contexts than the ones mentioned are considered not to be protected.

MAP-PP(2): Protection for Authentication Information including Handover Situations

This MAP-PP will protect Authentication information in all situations. The MAP dialogues identified by the application context and operations as well as their components within these dialogues subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:

Application Context/Operation	Protection Mode	Component	Protection Mode
infoRetrievalContext-v3/ Send Authentication Info	2	Invoke	1
		ReturnResult	2
		ReturnError	0
infoRetrievalContext-v2/ Send Authentication Info	2	Invoke	1
		ReturnResult	2
		ReturnError	0
infoRetrievalContext-v1/ Send Parameters (only if requested parameterList includes requestAuthenticationSet)	2	Invoke	1
		ReturnResult	2
		ReturnError	0
interVlrInfoRetrievalContext-v3/ Send Identification	2	Invoke	1
		ReturnResult	2
		ReturnError	0
interVlrInfoRetrievalContext-v2/ Send Identification	2	Invoke	1
		ReturnResult	2
		ReturnError	0
handoverControlContext-v3/ Prepare Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v3/ Forward Access Signalling (Note that the AC contains also other operations)	2	Invoke	2

handoverControlContext-v2/ Prepare Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v2/ Forward Access Signalling (Note that the AC contains also other operations)	2	Invoke	2
handoverControlContext-v1/ Perform Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v1/ Forward Access Signalling (Note that the AC contains also other operations)	2	Invoke	2

Additionally, MAP-PP(2) proposes the protection other critical MAP dialogues such us:

Application Context/Operation	Protection Mode	Component	Protection Mode
resetContext-v2/ Reset	1	Invoke	1
resetContext-v1/ Reset	1	Invoke	1

The rest of MAP dialogues identified by Application Contexts not included in this list are considered not to be protected. Also other operations within the listed Application Contexts than the ones mentioned are considered not to be protected.

MAP-PP(3): Protection for Authentication and Location Information

This MAP-PP will protect Authentication and Location information. The MAP dialogues identified by the application context and operations as well as their components within these dialogues subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:

Application Context/Operation	Protection Mode	Component	Protection Mode
infoRetrievalContext-v3/ Send Authentication Info	2	Invoke	1
		ReturnResult	2
		ReturnError	0
infoRetrievalContext-v2/ Send Authentication Info	2	Invoke	1
		ReturnResult	2
		ReturnError	0
infoRetrievalContext-v1/ Send Parameters	2	Invoke	1
		ReturnResult	2

(only if requested parameterList includes requestAuthenticationSet)		ReturnError	0
interVlrInfoRetrievalContext-v3/ Send Identification	2	Invoke	1
		ReturnResult	2
		ReturnError	0
interVlrInfoRetrievalContext-v2/ Send Identification	2	Invoke	1
		ReturnResult	2
		ReturnError	0
handoverControlContext-v3/ Prepare Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v3/ Forward Access Signalling (Note that the AC contains also other operations)	2	Invoke	2
handoverControlContext-v2/ Prepare Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v2/ Forward Access Signalling (Note that the AC contains also other operations)	2	Invoke	2
handoverControlContext-v1/ Perform Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v1/ Forward Access Signalling (Note that the AC contains also other operations)	2	Invoke	2
networkLocUpContext-v3/ Update Location (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
gprsLocationUpdateContext-v3/ Update GPRS Location (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	0
		ReturnError	0
handoverControlContext-v3/ Prepare Subsequent Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	0
		ReturnError	0
subscriberInfoEnquiryContext-v3/ Provide Subscriber Info	2	Invoke	1
		ReturnResult	2

		ReturnError	0
networkLocUpContext-v2/ Update Location (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v2/ Prepare Subsequent Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	0
		ReturnError	0
networkLocUpContext-v1/ Update Location (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	1
		ReturnError	0
handoverControlContext-v1/ Perform Subsequent Handover (Note that the AC contains also other operations)	2	Invoke	2
		ReturnResult	0
		ReturnError	0

Additionally, MAP-PP(3) proposes the protection other critical MAP dialogues such us:

Application Context/Operation	Protection Mode	Component	Protection Mode
resetContext-v2/ Reset	1	Invoke	1
resetContext-v1/ Reset	1	Invoke	1

The rest of MAP dialogues identified by Application Contexts not included in this list are considered not to be protected. Also other operations within the listed Application Contexts than the ones mentioned are considered not to be protected.

4 Discussion

Ericsson proposes to take the discussion on the level of definition for MAP-PPs presenting and balancing the pros and cons of each option.

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).

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 to save some processing capacity. However, this kind of MAP-PPs would introduce additional complexity to the system at the time of its definition, maintenance and configuration at peer NWs.

5 Summary and Conclusions

Ericsson does not consider definition of MAP-PPs per MAP-AC as the preferred option due to its poor granularity.

The option of MAP-PPs per MAP-Component is not seen as the best option either. As it can be seen from the previous chapters, the MAP-PPs come quite extensive even with limited number of operations if the MAP-PPs are defined on component level. Besides, taking a look to the proposed protection levels for each component, the claimed saving of processing capacity takes real relevance during error conditions (protected with PM0) which clearly represent a minimum percentage of the whole operation of the system.

Ericsson therefore proposes that operation level is chosen as the MAP-PP structure. This provides a perfect compromise between granularity and complexity while fulfilling security requirements. The added flexibility is not considered worth the complexity of management and implementation of MAP-PPs defined on component level.

However Ericsson kindly asks the members representing network operators to express their wishes on this issue.

Ericsson also asks SA3 to consider the content of the proposed Basic Protection Profiles presented in this contribution and further developed in the CR attached. If agreed, this CR shall be included in an updated version of TS 33.200.

3GPP TSG-SA WG3 Meeting #17 ***S3-010xxx***
Göteborg, Sweden, 27 February-2 March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **33.200** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **0.3.2** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	MAP Protection Profiles
Source:	⌘	Ericsson
Work item code:	⌘	Network Domain Security
Date:	⌘	27-Feb-01
Category:	⌘	**D**
Release:	⌘	Rel-4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	Include MAP protection profiles (Rel 4) in 33.200.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	7.2.7, Annex B.1		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

7.2.7 MAPsec protection profiles

MAPsec specifies a set of protection profiles. These profiles specifies the required protection level per MAP operation. The protection profile is then a set of attribute pairs (operation, protection level). Annex B.1 contains definitions for standard MAPsec protection profiles.

Table 3: Example of (Operation, Protection level) attribute pairs

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (authenticity/integrity and confidentiality)
AuthenticationFailureReport	1 (authenticity/integrity)
CheckImei	1 (authenticity/integrity)

The protection level for a specified operation applies for the operation irrespective of the dialogue/application context that the operation is part of. Corollary, a dialogue/application context may contain operations with different protection level. All components in a protected operation shall be protected with the same protection level.

NOTE: Operations shall have the same protection level for both the request and the response phase.

B.1 ~~UMTS Security~~Protection Profiles for MAPsec

MAP Protection Profile (MAP-PP) is an attribute in MAPsec Security Association. A MAP-PP defines the operations that shall be protected and the applied protection mode.

MAP-PP(0): No Protection

This MAP-PP does not contain any operation and it does not protect any information. This MAP-PP is used when no security is required or no security is an accepted option.

Operation	Protection Mode

MAP-PP(1): Protection for Authentication Information

This MAP-PP protects Authentication information in other than handover situations. The MAP operations subject to be protected and the corresponding Protection Mode to be applied are indicated in the table below:

Operation	Protection Mode
Send Authentication Info	2
Send Parameters (only if requested parameterList includes requestAuthenticationSet)	2
Send Identification	2

Additionally, MAP-PP(1) proposes to protect the following critical MAP operation:

Operation	Protection Mode
Reset	1

The rest of MAP dialogues carrying operations not included in this list are considered not to be protected.

MAP-PP(2): Protection for Authentication Information including Handover Situations

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

Operation	Protection Mode
Send Authentication Info	2
Send Parameters (only if requested parameterList includes requestAuthenticationSet)	2
Send Identification	2
Prepare Handover	2
Perform Handover	2
Forward Access Signalling	2

Additionally, MAP-PP(2) proposes to protect the following critical MAP operation:

Operation	Protection Mode
Reset	1

The rest of MAP dialogues carrying operations not included in this list are considered not to be protected.

MAP-PP(3): Protection for Authentication and Location Information

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

Operation	Protection Mode
Send Authentication Info	2
Send Parameters (only if requested parameterList includes requestAuthenticationSet)	2
Send Identification	2
Prepare Handover	2
Perform Handover	2
Forward Access Signalling	2
Update Location	2
Update GPRS Location	2
Prepare Subsequent Handover	2
Perform Subsequent Handover	2

Provide Subscriber Info	2

Additionally, MAP-PP(3) proposes to protect the following critical MAP operation:

Operation	Protection Mode
Reset	1

The rest of MAP dialogues carrying operations not included in this list are considered not to be protected.

~~[Editor: It seems unwise to proceed with the MAPsec profiles before we have a clear idea of what the MAPsec DoI RFC will contain.]~~

3GPP TSG-CN4 **Tdoc N4-010176**
CN#06 Meeting , Beijing, CHINA
15th January – 19th January 2001

Source: **TSG CN WG 4**

Title: **Proposed Response to SA3 on SA3 agreements on MAPSec**

To: **TSG SA WG3**

Contact Person:
Name: Peter Schmitt
E-mail Address: peter.schmitt@icn.siemens.de
Tel. Number: +49 6621 169 152

TSG CN WG4 thank TSG SA WG3 for their LS on SA3 agreements on MAPSec [S3-000760] and provide the following answers, comments, questions and information:

- **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.

- **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,
  - the key length which is to be mandatorily supported,
  - the mode of operation for AES which is to be mandatorily supported,
  - the mode of operation for AES-MAC which is to be mandatorily supported,
  - 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.

Specification of MAP-Protection Profiles
In addition to the alternatives given in the LS from SA3, protection Modes may also be specified against components of operations. This can be used to allow different components of the same operation, which are carried in different messages sent in different directions and thus being protected by different SAs, to be protected independently from each other.

If this alternative is chosen, CN4 proposes to standardise a limited number of profiles for Release 4. An example is given in the table:

Profile number	InfoRetrievalContext-v3			InterVlrInfoRetrievalContext-v3			AnyTimeInfoHandlingContext-v3		
	SAI invoke	SAI result	SAI error	SI invoke	SI result	SI error	ATM invoke	ATM result	ATM error
1	PM 1	PM 2	PM 0	PM 1	PM 2	PM 0	PM 1	PM 1	PM 0
2	PM 1	PM 1	PM 0	PM 1	PM 1	PM 0	PM 1	PM 1	PM 0
3	PM 2	PM 2	PM 0	PM 2	PM 2	PM 0	PM 2	PM 2	PM 0

SAI: SendAuthenticationInfo
SI: SendIdentification
ATM: AnyTimeModification
PM: Protection Mode

- **Use of Protection Mode 0**
  Protection mode 0 is relevant for cases where some but not all components need protection within a dialogue (e.g. error components). In cases where no component of a dialogue needs protection it is of course better and avoiding overhead not to make use of the MAP Security mechanism at all, rather than using the MAP security mechanism and "protecting" all components with protection mode 0.