3GPP TSG-SA3 Meeting #17 S3-010086
Göteborg, Sweden, 27th February- 2nd March 2001

Agenda Item: tbd (NDS WI)

Source: Siemens

Title: Protection Profiles for MAP Security

Document for: 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) Objection: It is not allowed to make the protection mode dependant from the content of the of the message SendParameters	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)Objection: It is not allowed to make the protection mode dependant from the content of the of the message SendParameters	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 (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
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

* MAP-PP per Component can be favoured because of following reasons:* This solution introduces no additional complexity as can be shown as follows:

As can be seen from the above Ericsson contribution no more than 3 or 4 combinations of protected modes are used de facto: These are : invoke/result/error: 1/1/0, 1/2/0, 1/0/0. We can define such a combination as a **protection level**. If we look at the complexity, maintenance and configuration, it makes no difference that we assign to an operation either 3 protection modes or assign it a protection level. The big benefit is however for the network signalling performance: We do not need to protect a response that does not include sensitive data, so in affect we do no need to transport needles bytes or do have needless security protection.

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 and suppliers 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.