3GPP TSG-SA3 Ad Hoc on 'Network Domain Security' **S3n010013**
Madrid 23-24 April, 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 have agreed on many issues related to securing MAP traffic on SS7 networks. The MAP Protection Profiles that are necessary to define which MAP payloads are in fact protected 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.

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 flexibility of applied security level and load optimisation. Complexity of implementation and management is not believed to be an issue here.

At S3#16 meeting, SA3 concluded that MAP-PPs both at MAP-AC level and MAP-Operation level were sufficient from a security point of view. 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 option allows for more flexibility and significant better performance while the level of security is not decreased, and the complexity for implementation and management is not increased.

3 Protection Profiles for MAP Security

3.1 Fallback to Unprotected Mode allowed Indicator

The "fallback to unprotected mode allowed 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, and not part of the MAP-PP. It is 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 proposed to define a limited number of "basic" MAP PPs.

A basic MAP Protection Profile (MAP-PP) is an attribute in a MAPsec Security Association. Several basic MAP-PP attributes may be attached to a MAPsec Security Association and thus form a complex Protection Profile for this SA. A basic MAP-PP defines for one or more MAP dialogues (identified by the application context and the first operation) whether protection is required. If so, it defines for every operation within this dialogue the protection level to be used.

Basic MAP PPs shall be defined in a non-overlapping way. This means that two “basic” MAP PPs shall not have the same set of application Context, Operation Mode and Protection Level values in common. This ensures that the complex MAP PP that is build by the initiating KAC to negotiate the MAP-SA in Phase 2, only contains the minimal needed information, therefor limiting the SA-negotiation complexity.

To allow for a simple management, the concept of "protection levels" is introduced: 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	2	0

Proposal for basic MAP-PPs:

MAP-PP(0): No Protection

This MAP-PP does not contain any application context. It is useful however to have a "null" MAP-PP to use on situations where no security is required or is an option. This basic MAP PP must not be combined with any other basic MAP PP.

MAP-PP(1): Protection of UMTS Authentication Information

This MAP-PP protects UMTS authentication quintets with protection mode 2 and requests for UMTS authentication quintets with protection mode 1. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
infoRetrievalContext-v3	Send Authentication Info	3
InterVlrInfoRetrievalContext-v3	Send Identification	3

MAP-PP(2): Protection of AnyTimeModification requests (a)

This MAP-PP protects AnyTimeModification request messages with protection mode 1. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
AnyTimeInfoHandlingContext-v3	AnyTime Modification	1

This basic MAP PP must not be combined with MAP-PP(3)

MAP-PP(3): Protection of AnyTimeModification requests (b)

This MAP-PP protects AnyTimeModification request messages with protection mode 2, and results of AnyTimeModification requests with protection mode 2. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
AnyTimeInfoHandlingContext-v3	AnyTime Modification	4

This basic MAP PP must not be combined with MAP-PP(2)

MAP-PP(4): Protection of Reset message

This MAP-PP protects Reset messages with protection mode 1. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
resetContext-v2	Reset	1
resetContext-v1	Reset	1

4 Discussion

Siemens 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 operations with a little security interest will still be protected although protection is not desired at the cost of additional processing capacity).

MAP-PPs per MAP-Operation would be still easy to define and maintain and would still provide poor granularity (MAP components with a little security interest will be protected although protection is not desired at the cost of additional processing capacity).

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; in other words Protection Level 3) this would allow to significantly save processing capacity. With the introduction of the concept of protection levels and the fact that de facto only three protection levels are used, this kind of MAP-PPs would still be easy to define and maintain.

5 Summary and Conclusions

a) The “fallback to unprotected mode indicator” is not considered to be part of a MAP-PP.

b) Only "basic" MAP-PPs shall be defined. Combinations of several basic MAP-PPs form complex MAP-PPs.

c) The concept of Protection Levels allows for easy definition, maintenance and configuration.

d) MAP-PPs are defined per MAP component.

Siemens does not consider definition of MAP-PPs per MAP-AC or per MAP-Operation as the preferred option due to their poor granularity and the resulting additional impact on processing capacity.

Siemens therefore proposes that component level is chosen as the MAP-PP structure. This provides the best granularity, the minimum impact on processing capacity and no additional complexity while fulfilling security requirements.

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

e) Scope for Rel-4 MAPsec shall be limited to MAP messages which require urgent protection.

These are MAP messages requesting or transporting UMTS Authentication quintets, and MAP messages requesting modification of a subscriber's data in the HLR and MAP Reset messages. By limiting the MAP messages that have protection in Rel-4, also the key management problem is kept controllable and may be done manually.

Siemens also asks SA3 to consider the content of the proposed Basic Protection Profiles presented in this contribution and in the CR attached. Siemens believe that these Protection Profiles cover all MAP messages that require urgent protection in Rel-4, and provide them with the most appropriate protection level. Additional Basic Protection Profiles covering less urgent MAP messages may be defined in Rel-5.

3GPP TSG-SA3 Ad Hoc on 'Network Domain Security' **S3n010013_attachment**
Madrid 23-24 April, 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:	⌘	Siemens
Work item code:	⌘	Network Domain Security
Date:	⌘	18-April-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 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:	⌘	Because the changes to Annex B.1 and 7.2.7 are very extensive (i.e. include a lot of new text), Siemens decided not to use change bars to the original draft TS 33.200 V0.3.2.

7.2.7 MAPsec protection profiles

MAPsec specifies a set of protection profiles. These profiles specify the required protection level per MAP operation. The protection profile is a set of attribute pairs (operation, protection level). Annex B.1 contains definitions of basic protection profiles. A list of basic protection profiles forms a complex protection profile.

B.1 Protection Profiles for MAPsec

A basic MAP Protection Profile (MAP-PP) is an attribute in a MAPsec Security Association. Several basic MAP-PP attributes may be attached to a MAPsec Security Association and thus form a complex Protection Profile for this SA. A basic MAP-PP defines for one or more MAP dialogues (identified by the application context and the first operation) whether protection is required. If so, it defines for every operation within this dialogue the protection level to be used. The protection level of an operation within a protected dialogue defines the applied protection modes for every component (invoke, result, error) of the operation 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	2	0

The following basic MAP-PPs are defined:

MAP-PP(0): No Protection

This MAP-PP does not contain any application context. It is useful however to have a "null" MAP-PP to use on situations where no security is required or is an option. This basic MAP PP must not be combined with any other basic MAP PP.

MAP-PP(1): Protection of UMTS Authentication Information

This MAP-PP protects UMTS authentication quintets with protection mode 2 and requests for UMTS authentication quintets with protection mode 1. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
InfoRetrievalContext-v3	Send Authentication Info	3
InterVlrInfoRetrievalContext-v3	Send Identification	3

MAP-PP(2): Protection of AnyTimeModification requests (a)

This MAP-PP protects AnyTimeModification request messages with protection mode 1. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
AnyTimeInfoHandlingContext-v3	AnyTime Modification	1

This basic MAP PP must not be combined with MAP-PP(3)

MAP-PP(3): Protection of AnyTimeModification requests (b)

This MAP-PP protects AnyTimeModification request messages with protection mode 2, and results of AnyTimeModification requests with protection mode 2. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
AnyTimeInfoHandlingContext-v3	AnyTime Modification	4

This basic MAP PP must not be combined with MAP-PP(2)

MAP-PP(4): Protection of Reset message

This MAP-PP protects Reset messages with protection mode 1. The MAP dialogues identified by the application context and the operations subject to be protected and the corresponding Protection Levels to be applied are indicated in the table below:

Application Context	Operation	Protection Level
resetContext-v2	Reset	1
resetContext-v1	Reset	1