3GPP TSG SA WG3 Security — S3#16 **S3-000673**

Sophia Antipolis (France), 28th-30th November, 2000

Agenda Item: 10.7

Source: Ericsson

Title: Protection Profiles for MAP Security

Document for: Information and Discussion

1 Introduction

This contribution presents the different alternatives for the specification of the internal structure of Protection Profiles for MAP Security.

S3 members are kindly requested to discuss these different alternatives in order to take a decision on what is the best approach to be followed.

2 Background

During the discussion of documentsS3z000014 (Ericsson) and S3z000031 (Siemens) at S3#15bis meeting (8th-9th November), different positions on the specification of MAP-PPs were presented and discussed.

The most controversial issue was the specification of the internal structure of MAP-PPs (Protection Modes vs MAP-Operation/AC/Component?).

3 Alternatives for Specification of MAP-PPs

Ericsson contribution S3z000014 proposes that the specification of Protection Profiles for MAP Security should indicate protection modes per MAP Operation:

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

Siemens proposed that Protection Modes should be specified against MAP Application contexts and going down a step further also consider the specific MAP Component within the MAP Dialogue:

Application Context	Component	Protection Mode
InfoRetrievalContext-v3	SendAuthenticationInfo Invoke	0 or 1 (tbd)
	SendAuthenticationInfo ReturnResult	2
	SendAuthenticationInfo ReturnError	0

There could even be a third approach where Protection Modes are specified against MAP Application Contexts only:

Application Context	Protection Mode
InfoRetrievalContext-v3	2 (authenticity/integrity and confidentiality)

3.1 Protection Modes per MAP Operation

Having previously agreed to base the structure of secure MAP on a per MAP Operation basis (agreement of S3z000013 at S3#15bis ad-hoc meeting in Munich), it is Ericsson's understanding that the most suitable way to define Protection Modes would be also based on a MAP Operation basis.

From an stage 2 specification point of view this should be enough in order to provide manufacturers and other standardisation groups (i.e. CN4) accurate requirements for its correct handling and implementation.

3.2 Protection Modes per MAP Component

Siemens approach allows the definition of different Protection Modes for the different components of a MAP Operation.

To this respect, Ericsson would like to point-out that once it has been decided to protect the dialogue in which a MAP operation takes place, it seems much more natural, reasonable and simpler to offer the same level of protection during the whole dialogue.

It shall also be considered that, although from an implementation point of view, this flexibility could be offered, network operators might never use it. They would rather prefer to define the same level of protection for the different components of a MAP Operation, thus having a rather simpler and easier to maintain MAP-PP structure.

3.2 Protection Modes per MAP Application Context

Regarding the alternative approach that proposes the use of MAP-ACs instead of MAP Operations, it shall be noted that this is quite suitable in the case MAP-ACs comprised one single MAP Operation (e.g. infoRetrievalContext-v3 = sendAuthenticationInfo).

However, this is not always the case. As an example MAP-AC "networkLocUpContext" comprises the following MAP Operations:

- updateLocation
- forwarCheckSs-Indication
- restoreData
- insertSubscriberData
- activateTraceMode

The Protection Mode applicable to these kind of Application Contexts, shall be the one of the MAP Operation within the Application Context requiring the highest level of protection. In the case of the example above, MAP-AC "networkLocUpContext" would be assigned a Protection Mode 2 corresponding to the protection level required by the MAP Operation "updateLocation".

This may lead to the case where an specific MAP Operation is given an specific protection mode while, from a security point of view, that MAP Operation requires a lower level of protection ("insertSubscriberData" requires Protection Mode 1) or not protection at all ("activateTraceMode").

Besides, the use of MAP-ACs and their different versions introduce additional complexity in the handling of MAP-PPs.

4 Conclusion

S3 members are kindly requested to discuss these different alternatives taking into consideration the pros and cons of each approach, in order to take a decision on what is the best one to be followed. In particular, the opinion and preferences from S3 members representing network operators is essential in order to have a clearer view on the requirements for the handling of MAP-PPs.

Corresponding agreements (if any) reached during S3#16 regarding this issue shall be incorporated to TR 33.800. Later on, actual proposals of Basic MAP-PPs shall be presented and considered in TS 33.xxx on “Network Domain Security”.

It must also be noted that the decision reached at S3 regarding the structure of MAP-PPs may have an impact on working assumptions currently followed at CN4 and therefore this group shall be liaised after the discussion at S3#16 regarding this issue.