

Agenda Item: tbd (NDS WI)
Source: Siemens
Title: Comments on TS 33.200 v050
Document for: Discussion and Decision

1 Scope and Objectives

This contribution summarizes the Siemens comments on TS 33.200 v050.

After a Siemens internal review, it was clear that the TS 33.200 v050 still needs to be changed a lot, and therefore Siemens opted to submit a contribution that summarizes the review comments, rather than detailing each them. We think that this is a more efficient way of handling given the current state of the specification. It must also be noted that this contribution does not sum up all technical open issues (A first attempt was done at the S3 adhoc in Madrid), but its content is related to the main editorial remarks we found.

2 Comments on TS 33.200 v050.

A) Not all Rel5 content has been removed

There are still several parts of the document that contain Rel5 definitions (RequestSA, KAC, ..) and content. Examples are section 4.2 (discussion on several KACs), and section 5.2 (and possibly others).

It is proposed to review the document accordingly and remove all Rel5 material from the normative sections.

B) The MAPsec DoI is not relevant for Rel4

Section 5.3 is about the MAPsec DoI. In our view, the current MAPsec DoI should not be of any relevance for Rel4. Furthermore, the MAPsec DoI is currently in the state of an IETF draft and being reworked currently, so it cannot be used as a reference in a 3GPP TS document anyway. A Rel4 specification shall rely on the definition of the MAPsec SA, and the procedures how to handle it.

Therefore section 5.3 shall be cleaned from the MAPsec DoI parts and renamed.

C) Review/Cleanup of annex A, B, C

People who read the final TS will probably read the annex as well. Therefore, in this annex everything that is not regarded as relatively stable or agreed in principle by SA3 should be removed. Although informative, the annex is part of a TS document and should not be in an inconsistent state (note, that the Madrid SA3 ad-hoc meeting proposed to drop TR 33.800 for exactly this reason).

Therefore, it is proposed to do a careful review of the annex sections.

Section A.3.4 (MAP SA information) does not belong into an informative annex. This should be part of the main document.

D) MAP SA definition is incomplete.

The MAP SA definition in section 5.3.2 is still incomplete and has to be completed. It is proposed to review the MAP SA definition of annex A.3.4 for this purpose.

E) Algorithm and mode selection must be completed.

Section 5.6, MAPsec algorithms, is still incomplete. For encryption, the algorithm (AES mode of operation, block or stream cipher) has to be chosen. For both the integrity algorithm and the encryption algorithm, a definition is required.

F) MAP protection Profiles and Protection Groups needs to be evaluated.

The editor of TS 33.200 did mention that the section 6 is in a draft-status originating from the S3 adhoc on NDS security. SA3 shall cleanup this section according to the recommendation on MAP operation or component level that will be given by N4. Furthermore a threat assessment is needed to select only the MAP-operation that really need protection. It is suggested to use tdoc AP99-028 (SS7 NETWORK SECURITY THREAT ANALYSIS) for these purposes. On this basis adequate Protection Groups can be build that can be combined towards Protection Profiles.

G) Definitions clarification needed.

Definitions have to be clarified. Examples are Local key distribution, UMTS network Domain, manual Interdomain SA.

H) Is interfaces table 2 normative or informative ?

Table 2 at section 4.4 describes the interfaces that are effected by the network domain security. It shall be clarified what the normative meaning is of this table against the definitions of protection profiles.

I) Fallback to unprotected Mode Indicator and MAP SA handling for Rel4 missing.

The document needs to have a normative part that describes how the fallback indicator is going to be used and how the MAPsec SA is going to be handled in the MAP NE. A suggestion is to start with the contents of section A.3.1/A.3.2 and remove all Rel5 indications.

3 Conclusions

Still a lot of work is needed to incorporate the main editorial comments and to solve the outstanding technical issues at the SA3#18. Therefore Siemens recommends an additional review on the TS 33.200 after SA3#18 to check the inclusion of the technical progress and the editorial changes discussed at the SA3#18, before the Technical Specification could be sent to the SA-plenary.