ERICSSON

S3-020273

Notes from IMS Drafting Session

Krister Boman
Ericsson

ERICSSON

Results from the Drafting Session:

- For Release 5 only integrity protection shall be required and to make it easier to extend this in Release 6 the Null algorithm for encryption shall be included in the list from the UE
- Separate SAs are required for TCP and UDP
- The same integrity key shall be used in both directions and for TCP and UDP. In order to mitigate the reflection attack the SPIs shall be different as proposed in TDOC 234.
- The majority of the group did not see the need for a key derivation mechanism for Release 5. In order to expand a 128 bit integrity key for SHA1 the 32 first bits of the IK shall be appended to IK itself
- HMAC for MD5 and SHA1 shall be supported in Release 5

ERICSSON

Results from the Drafting Session:

- The majority of the group supported that the SA lifetime shall be controlled at SIP layer and that at IPSec layer the SA lifetime is set to 2^{32}-21 seconds. This shall be adopted if no alternative CR is presented challenging this proposal at this meeting. Some security concerns were raised and every participant is encouraged to investigate if there are any security weaknesses with this proposal.
- Only one registration is allowed per user at a time. Hence no more than three SAs are required at the most.
- The current proposal introducing the concept of suites for IPSec need to be updated such that the agreed working assumptions are reflected accurately

ERICSSON

Results from the Drafting Session:

- An attack has been identified in TDOC 234 and different alternatives are currently discussed. Günther will draft an LS to CN1 in order to conclude if the Contact can be used. Another potential solution could be to send the IP Address in SM7 by using the implementation of the SIP Sec Agree.
- It was concluded that given that we should be ready on Wednesday such that an LS can be sent to CN1 a drafting session is likely to be required in order to align the agreed CRs into one ‘big’ CR which can be approved at this meeting.

ERICSSON

Results from the Drafting Session:

- Question 1: Is it possible to send information like e.g. SPI which is dynamic in a static list in SIP Sec Agree? ***Yes***
- Question 2: Is it possible to send the IP Address of the UE protected by the third message utilising SIP Sec Agree? ***Shall be investigated further.***