Revised Recommendations in respect of WP/3-13, "Overall Security Concept", relating to the work of WG2

Recommendation 2 - Protection of the Routing Information Base

It is recommended that WG2 be asked to investigate means by which the routing information base should be protected from unauthorised modification, through the unauthorised use of IDRP, with the objective of specifying a suitable mechanism in the context of CNS/ATM-2 package and beyond. Such unauthorised modification may result in "Denial of Service" to ATN internet users.

WG2 is invited to comment on the suitability of the Digital Signature Standard described in section 4.1.1 to achieve this.

Recommendation 6 - Protection of Systems management Messages

It is recommended that WG2 be asked to investigate means by which systems management messages should be protected against modification, masquerade and replay, with the objective of specifying a suitable mechanism in the context of CNS/ATM-2 package and beyond. The protection mechanism needs to ensure:

a) it shall not be possible to modify (without detection) a message once it has been produced
b) it shall always be possible to tell reliably from a message who the original sender was
c) it shall be possible to recognise the correct sequence of messages, so that if a message is received out of sequence, this fact is recognisable.

WG2 is invited to comment on the suitability of the Message Authentication Check (MAC) mechanism identified in section 4.2 to achieve this.

In the context of both the above, WG2 is invited to note that in its work on the Overall Security Concept, WG1 intends to carry out further research into suitable encryption algorithms for use within the ATN, and into the issues associated with key distribution.