SAP Security Update

Colin Perkins <c.perkins@cs.ucl.ac.uk>
University College London
Gower Street
London WC1E 6BT

Overview

- Provide mechanisms for authenticated and private announcements
- Symmetric: DES
- Asymmetric: PGP, PKCS#7
- Last draft was draft-ietf-mmusic-sap-sec-04

Changes since last draft

- Signature length field was PGP specific
  - Moved into from main authentication header to PGP sub-header
- Standard privacy header for all types of encryption
  - Previously symmetric & asymmetric algorithms used different headers

To do

- SAP version number
  - Should increment since inclusion of privacy header for symmetric is not backwards compatible?
- Merge with main SAP specification
  - Work in progress