SAP Security

Colin Perkins <c.perkins@cs.ucl.ac.uk>

Department of Computer Science

University College London

Gower Street

London WC1E 6BT

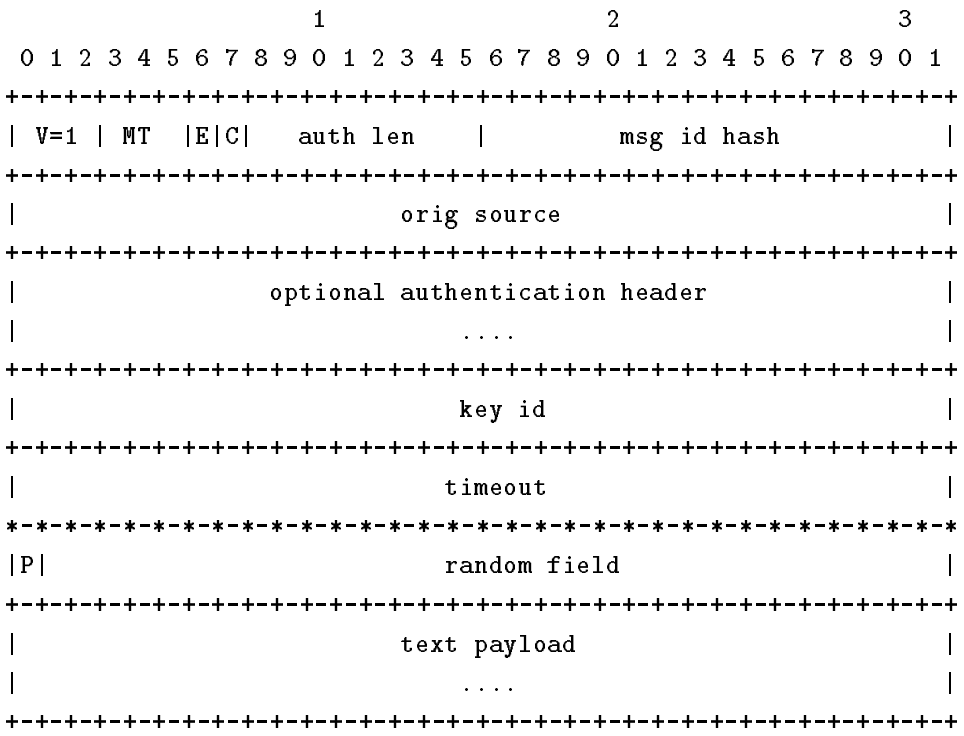
SAP Limitations

draft-ietf-mmusic-sap-00 is weak on security

- Privacy using symmetric encryption (eg: DES)
- Authentication hooks are present, but details are not specified

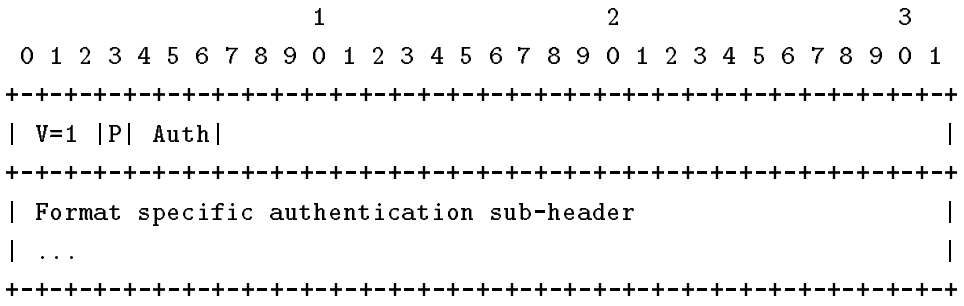
draft-ietf-mmusic-sap-sec-00 specifies the SAP authentication and privacy headers using either PGP or "simple public key format" (loosely based on PKCS#7)

Encrypted SAP Packet Format



Authentication

Generic authentication header, followed by specifics depending on the algorithm chosen:



The "Auth" field specifies the algorithm used and format of the sub-header.

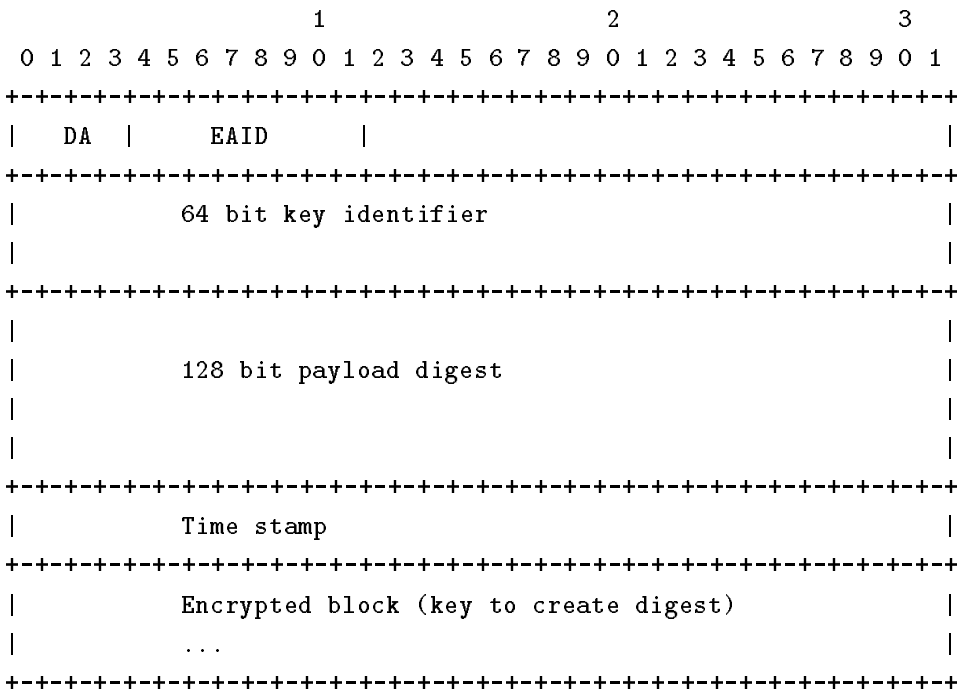
Can be either PGP or 'Simple public key format', with either the public key, key ID, or certificate included.

Authentication: PGP

The PGP authentication sub-header contains a PGP digital signature packet, as in RFC1991.

In addition, a public key packet or a certificate packet may be included if required.

Authentication: Simple Public Key Format



DA = Digest algorithm; EAID = Encryption algorithm

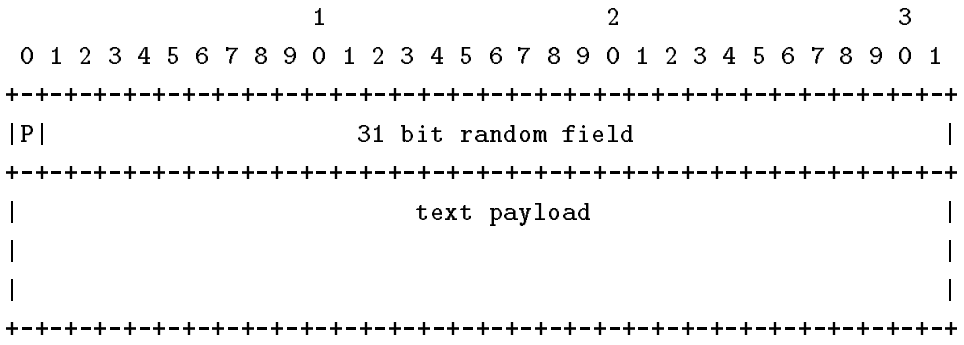
Privacy

There is currently no generic privacy header: format depends on the encryption algorithm used.

Question: should we define a generic privacy header, giving algorithm used?

Privacy: Symmetric Encryption

For symmetric encryption we follow the SAP draft: prepend a 32 bit field comprising a 31 bit random number, and a single padding bit.

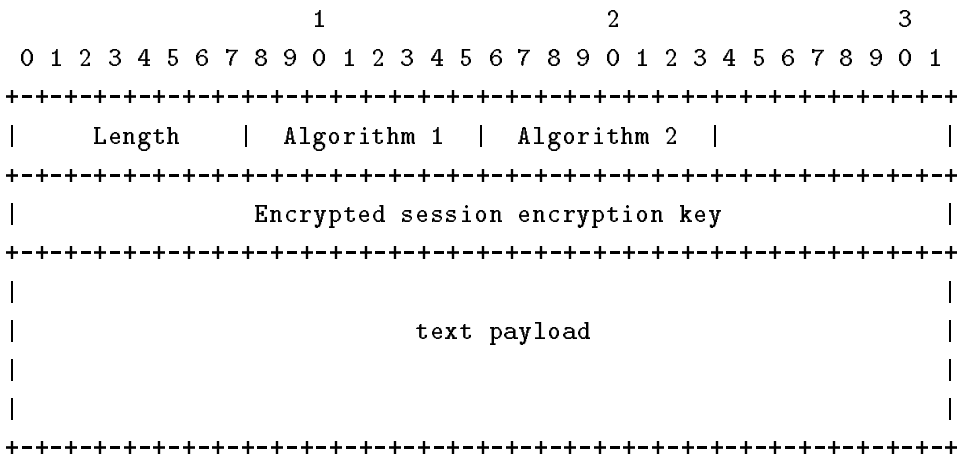


Privacy: PGP

The privacy header for PGP format is a standard PGP public key encrypted packet, as in RFC 1991.

This is followed by the encrypted payload, encapsulated as for PGP.

Privacy: Simple Public Key Format



The algorithm fields indicate the asymmetric algorithm used to encrypt the session key, and the symmetric algorithm used to encrypt the payload.

Open Issues

- Is the key ID field in the main SAP header required?
  - Weakens symmetric encryption
  - Both PGP and PKCS#7 have key ID fields within their packet
- Define a standard privacy header, detailing algorithms used?
- Use "simple public key format" or full PKCS#7?