

# AVTP Security Format

Dave Olsen/Jeff Koftinoff

6/25/12

# Security Header (old)

- Reserved (4 bytes)
- EUI-64 – Signature Key ID (8 bytes)
- EUI-64 – Encryption Key ID (8 bytes)
- Signature (32 bytes)
- Magic Number (4 bytes)
  - Is there a standard we can point to? (MikeJT)
- Random Data (8 bytes)
  - Is there a standard we can point to?
  - EMSA4 (12.1.4 IEEE 1363a) (need to request 1363a)

# Security packet types

- Every type begins with 4 bytes of reserved data
- Define something in the 4 bytes to distinguish packet header type
  - 1) Signed Packet Header
  - 2) Encrypted Packet Header
  - 3) No security

# Signed Packet Header

- Reserved (4 bytes)
- EUI-64 – Signature Key ID (8 bytes)
- Signature (32 bytes)

# Encrypted Packet Header

- Reserved (4 bytes)
- EUI-64 – Encryption Key ID (8 bytes)
- Magic Number (4 bytes)
  - Is there a standard we can point to? (MikeJT)
- Random Data (8 bytes)
  - Is there a standard we can point to?
  - EMSA4 (12.1.4 IEEE 1363a) (need to request 1363a)

# No Security Packet Header

- Reserved (4 bytes)

# Version 1 header format

- Insert the security header before the Stream ID
- Version 0 and Version 1 continue to be supported formats
- Once a stream is setup all stream packets must use the same Version 1 header
  - Streams are required to use the same security header through the life of the stream
  - Control Packets are free to intermix security types, although this may not be desirable

# Draft modifications

- This will require rework of all the common header formats for version 1
- All other packet types will need to be described as a generic header plus content
- 1722.1 has already done this and we should follow their example.



# References

- IEEE 1363 defined key exchange
- Data is AES-128
- FIPS 197