MSEC WG Meeting (IETF-63) - Paris

draft-cruickshank-ipdvb-sec-00.txt
ULE security extensions

Authors: Haitham Cruickshank and Sunil Iyengar *(University of Surrey, UK);*
Stephane Combes and Laurence Duquerroy
(Alcatel Alenia Space, Toulouse, France)

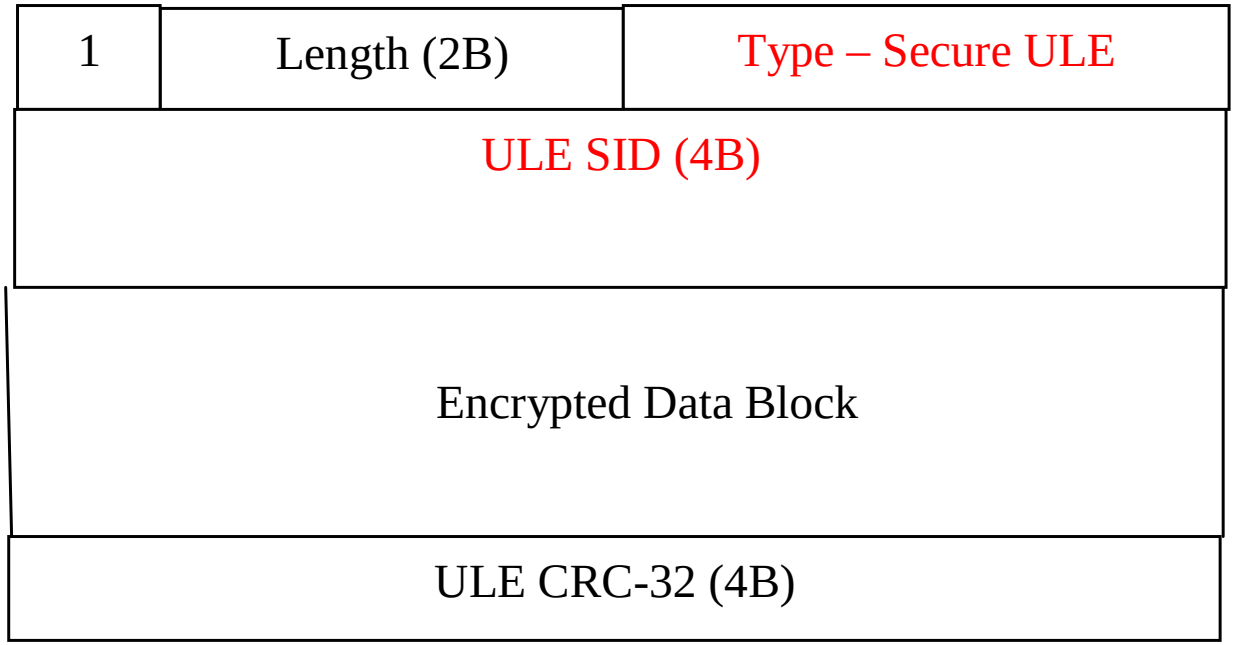
Why do we need ULE (link layer) security

- This is an additional security mechanism to IP and above layers; not a replacement:
  - For example it can work in parallel with IPsec.

- Motivations:
  - Ability to provide security by the wireless/satellite operator in relation to controlling access to the service.
  - Capability to work with non-IP packet formats
  - Protect of identity of the Receiver within the MPEG-2 transmission network.
  - Transparency to the use of Performance Enhancing Proxies, where IPsec can not be used.

UniS

SNDU Format for Encryption Header



- A new ULE Mandatory Extension header for encryption:
  - The ULE Security IDentifier (ULE-SID) is a 32 bit value (similar to the IPsec SPI).
  - The ULE-SID can be used by a Receiver to filter PDUs in conjunction with the set of MAC/NPA addresses that it wishes to receive.

MSEC compatibility issues…

- Encryption algorithms, key lengths...
  - use of the standard IPsec and msec suites.
- key space
  - Re-use IPsec msec key databases
- Comments from msec on possible problems and incompatibility issues.