#### IPDVB WG Meeting (IETF-66) - Montreal

# draft-cruickshank-ipdvb-sec-02.txt

# **Security Extension for ULE**

Authors: H. Cruickshank (University of Surrey, UK),
P. Pillai (University of Bradford),
S. Iyengar (University of Surrey, UK) and
L. Duquerroy (Alcatel Alenia Space, Toulouse, France)



### Draft status - 1

- Document describes the extension format for ULE that secures the IP traffic/Bridged Ethernet frames transported using ULE
- Based on the security requirements ID
  - draft-cruickshank-ipdvb-sec-req-02.txt
- Describes processing of security extension header at ULE Encapsulator and Receiver.



### Draft status - 2

- It uses a subset of standard IPsec databases entities (SPD and SAD). A new entry is needed:
  - Network Point of Attachment (NPA): An address may identify individual Receivers or groups of Receivers
- Key management alternatives:
  - Network layer: Existing key management systems can be used such as the MSEC key exchange protocols, GDOI and GSAKMP. The format of the ULE-SID will be identical to the security association as defined in GDOI or GSAKMP.
  - Other key management systems such as link layer systems (e.g. DVB-RCS)



## General SNDU format with Security

```
Length
                                   Type = S-ULE
           Receiver Destination NPA Address *
                                  ULE_Security_ID
    ULE_Security_ID
                                 Sequence Num.(Optional)
Sequence Number (Optional)
                                    MAC (Optional)
     MAC (Optional)
                             Type = Type of PDU
                      Encrypted PDU
                 Cyclic Redundancy Code
```

#### **Detailed Secure ULE SNDU format with D=0**

```
Length (15 bits)
                                 Type = S-ULE
  Temporary Receiver Destination NPA Address (48 bits)
                                  ULE_Security_ID
                                Sequence Num. (Optional)
    ULE_Security_ID
Sequence Number (Optional)
                                    MAC (Optional)
     MAC (Optional)
                              Type = Type of IPv4
                Encrypted IP Datagram
            Cyclic Redundancy Code (32 bits)
```

## Detailed Secure ULE SNDU format with D=1

```
Length (15 bits)
                     Type = S-ULE
            ULE_Security_ID
          Sequence Number (Optional)
  Message Authentication Code (Optional)
 Type = IPV4
           Encrypted IP Datagram
           Cyclic Redundancy Code
```



# Discussions on the ipdvb mailing list

### • George Gross:

- It fits the requirements ID
- More detailed description of ULE-SPD
- Security protections for the inverse SNDU traffic flow
- Multiple sender issues
- Tesla for source authentication



## Future plans

- Incorporate all comments to a new draft:
  - Hopefully this work will be adopted as work item for ipdvb WG
  - Produce new draft within a month.
- Implement this work by the end of year by:
  - The authors
  - Collaboration with other ipdvb WG members

