IPDVB WG Meeting (IETF-72) - Dublin

draft-cruickshank-ipdvb-sec-05.txt

Security Extension for ULE

Authors: H. Cruickshank and (University of Surrey, UK); P. Pillai (University of Bradford) and S. Iyengar (Logica, UK)

Draft status

- Document describes the extension header format for ULE. It is based on the security requirements ID:
 - draft-ietf-ipdvb-sec-req.txt (latest version 08)
- It presents the processing of security extension header at ULE Encapsulator and Receiver.
- It uses a subset of standard IPsec databases (SPD and SAD). Various key management schemes can be used.
- Partial implementation exists.
- Future plans are to complete coding and publish as open source code.



General SNDU format with Security

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5	678901234567890	1
D Length	Type = S-ULE	Ĭ
Receiver Destinat	tion NPA Address *	
 	ULE_Security_ID	
ULE_Security_ID	Sequence Num.(Optional)	<u> </u>
Sequence Number (Optional)	MAC (Optional)	
MAC (Optional)	Type = Type of PDU	<u> </u>
Encrypted PDU		 -
Cyclic Redundancy Code		Jni