DTLS over DCCP

Tom Phelan

tphelan@sonusnet.com

draft-phelan-dccp-dtls-00.txt

Background

- Transport Layer Security (TLS)
  - Encryption/authentication built just above the transport layer
  - Uses TCP as transport
- Datagram Transport Layer Security (DTLS)
  - TLS depends on TCP’s reliable delivery service
    - For initial connection setup/keying handshake
    - For decryption of data (state depends on previous data)
  - DTLS adds reliability to connection handshake and makes decryption independent of previous data
  - Uses UDP as transport

DTLS over DCCP

- Simple approach
  - DTLS records are sent in DCCP-Data packets
    - As with UDP, multiple records allowed in one DCCP-Data if fit
- Some enhancements
  - DTLS handshake MAY use DCCP-Request and DCCP-Response Application Data
  - PMTUD SHOULD be done by DCCP

Next Steps

- Draft silent on use of service codes
  - Propose to add:
    - An application using DTLS over DCCP SHOULD register a new service code for the combination, but MAY use the same service code as when operating without DTLS.
- Tracking changes to DTLS
  - What happens to DTLS over DCCP when DTLS goes to next version?
- ??