16-124-836
Marcel Matti ZAUDER

10.3 Question 3

10.3.A Which of the following features are provided by both TLS and DTLS, and which only by DTLS? For those provided only by DTLS, explain why they are needed in DTLS and not in TLS.

Confidentiality, integrity

Both

Message fragmentation and reassembly in the Handshake Protocol

Only DTLS uses this as the handshake messages may exceed the natural datagram length.

Alert messages (*unknown_ca*, *certificate_expired*, …)

Both

Key exchange

Both

Cookie exchange

Only DTLS uses this feature in order to provide a protection against DoS or spoofing attacks. After the ClientHello the server responds with a HelloVerifyRequest which contains an opaque cookie. This cookie must be send back by the client as a second ClientHello.

Retransmission of lost handshake messages

As DTLS accepts datagrams to be lost, duplicated, or reordered, DTLS implements a handling of this alterations.