CS8601 –MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.4. Wireless transport layer security (WTLS)

The wireless transport layer security (WTLS) can be integrated into the WAP architecture on top of WDP. Supports datagram and connection-oriented transport layer protocols. Based on TLS/SSL protocol.

Provide different levels of security for:

- Privacy
- Data integrity
- Authentication

Optimized for low bandwidth, high-delay bearer networks.

Takes into account:

- Low processing power
- Limited memory capacity

Before data can be exchanged via WTLS, a secure session has to be established. Both originator & peer can interrupt the session at any time.

Steps in the Session establishment:

Step 1: Negotiation of the security parameters and suites:

1.1.Initiate the session with the SEC-Create :

- SA: Source Address
- SP: Source Port
- DA: Destination Address
- DP: Destination Port
- KES: Key Exchange Suite (e.g. RSA, Diffie, ECC)
- CS: Cipher Suite (e.g. DES, IDEA)
- CM: Compression Method

1.2The peer answers with parameters:

- SNM: Sequence Number Mode
- KR: Key Refresh Cycle (how often the keys are refreshed within this secure session)
- SID: Session Identifier (unique for each peer)
- KES': Key Exchange Suite (e.g. RSA, Diffie, ECC)
- CS': Cipher Suite (e.g. DES, IDEA)
- CM': Compression Mode

Step 2: Peer also issues SEC-Exchange:

Indicate that peer wishes to perform public-key authentication i.e., peerrequests a certificate from the originator.

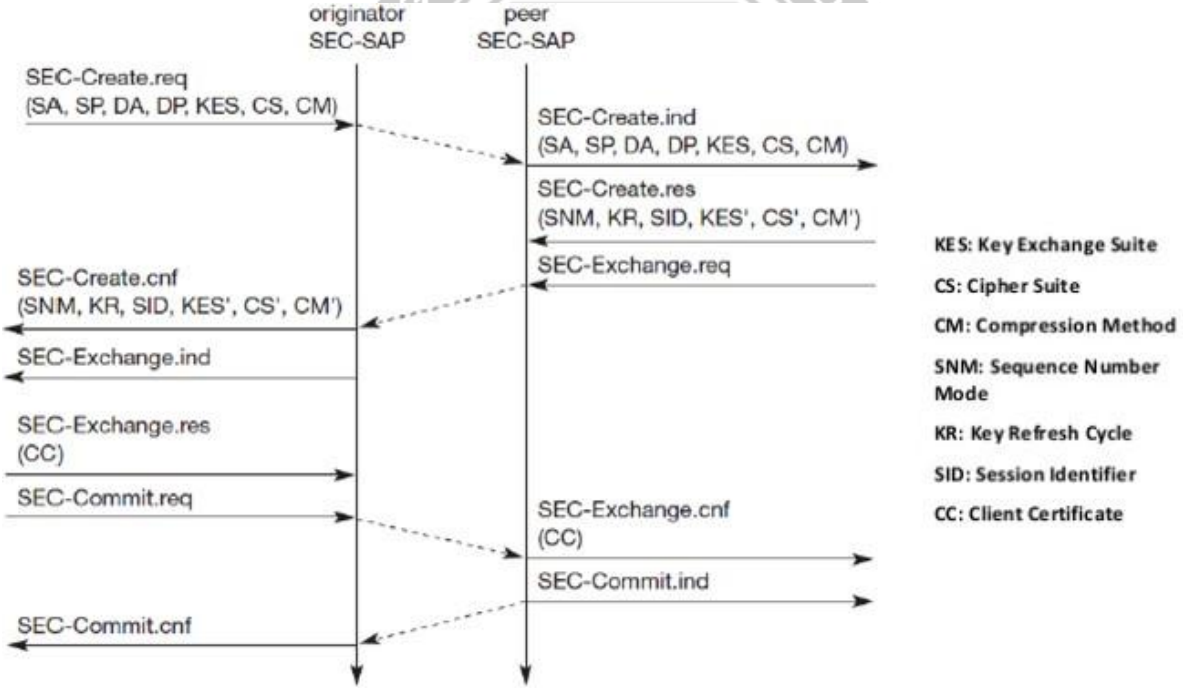

Fig. WTLS establishing a secure session

Step 3: The originator issues SEC-Commit.req:

- The originator answers with its certificate.
- Indicates that the handshake is complete.

Step 4: SEC-Commit.ind :

- Indicates that the certificate is delivered
- Concludes the full handshake.

Step 5: User datagram can be exchanged using SEC-Unitdata:

- Same function as T-DUnitdata on the WDP layer

The parameters are the same here:

source address (SA), source port (SP), destination address (DA), destination port (DP), and user data (UD)