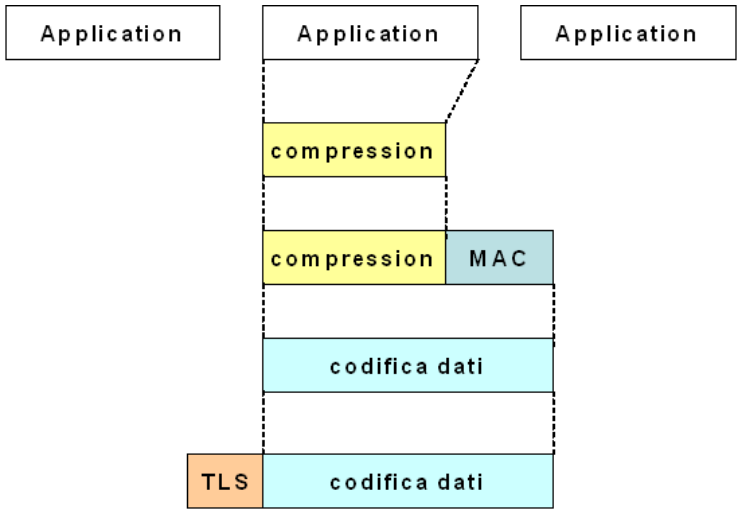
SSL TLS record

La lunghezza massima di un record SSL = 16384 byte (RFC 2246); il protocollo SSL/TLS prevede che ogni messaggio di handshake sia contenuto in un unico record SSL, mentre i dati provenienti dalle applicazioni possono essere anche frammentate in più record SSL.



Per evitare complicazioni di critto-analisi è prevista la possibilità di comprimere i dati prima di codificarli; inoltre prima della codifica è previsto il calcolo di un codice MAC che agisce come segnatura del messaggio (garantisce l'originalità dei dati).

L'operazione di codifica viene effettuata utilizzando un algoritmo simmetrico ed uno schema CBC (Cipher Block Chaining) per la codifica di messaggi lunghi.

Il calcolo del MAC avviene utilizzando la seguente formula:

H (write_MAC_secret + pad2 + H (write_MAC_secret + pad1 +seq_num + type + length + data))

dove:

- **H:** generica funzione di digest
- **write_MAC_secret:** rappresenta una delle chiavi associate alla connessione, condivise tra le due entità SSL/TLS
- **pad1:** è il carattere esadecimale 0x36 ripetuto 48 volte se si usa funzioni digest MD5, 40 volte se utilizza SHA
- **pad2:** è il carattere esadecimale 0x5c ripetuto 48 volte per MD5, 40 volte per SHA
- **seq_num:** è il sequence number che identifica la posizione del messaggio all'interno del flusso di dati scambiati tra entità SSL
- **type, lenght e data:** rappresentano rispettivamente il tipo di protocollo trasportato, la lunghezza del messaggio ed i dati dopo la compressione prevista dal protocollo TLS record.

Terminata la codifica del messaggio il protocollo TLS record provvede ad aggiungere un'intestazione contenente le seguenti informazioni:

- **content type:** indica la natura dei dati trasportati
- **protocol version:** indica la versione del protocollo
- **lenght:** indica la lunghezza del record.

Il corpo vero e proprio del record SSL/TLS è invece costituito da:

- **Data Payload:** contiene le informazioni trasportate
- **MAC: (**opzionale) contiene la segnatura del messaggio
- **Padding Data:** (opzionale)