**Secure Socket Layer / Transport Layer Security**

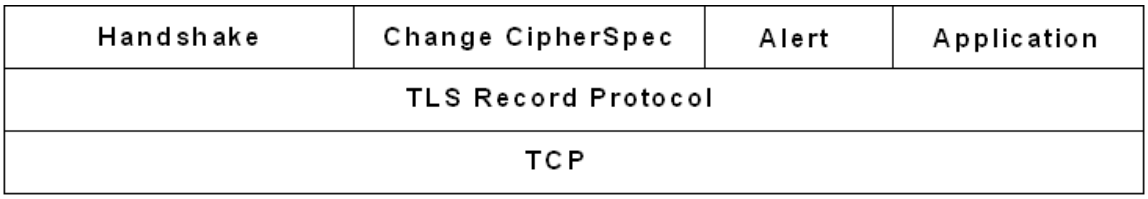
Per ottenere la negoziazione di funzioni crittografiche sicure e trasparenti all'utente è indispensabile che le applicazioni riconoscono in maniera automatica quando ricorrere alle funzionalità del protocollo SSL/TLS; per questo motivo la IANA ha definito le porte **TCP** riservate ai servizi tradizionali fruiti tramite **SSL/TLS.**

| Protocollo | Porta standard | Porta SSL |
|---|---|---|
| HTTP | 80 | 443 |
| NNTP | 119 | 563 |
| LDAP | 389 | 636 |
| FTP data | 20 | 989 |
| FTP control | 21 | 990 |
| TELNET | 23 | 992 |
| IMAP | 143 | 993 |
| IRC | 194 | 994 |
| POP3 | 110 | 995 |
| SMTP | 25 | 465 (revoked); 25/tcp (RFC 3207) |

Il ruolo del protocollo SSL/TLS è creare un canale sicuro per la trasmissione dei dati:

- garantire la riservatezza dei dati trasmessi tra applicazioni client e server
- autenticare il lato server ed occasionalmente autenticare il lato client
- la negoziazione di un opportuno sistema crittografico
- lo scambio delle chiavi necessarie sulla base dello schema crittografico selezionato
- l'autenticazione dei partecipanti
- la codifica di tutti i messaggi scambiati tra i partecipanti.

**Architettura SSL/TLS**




I parametri che contraddistinguono una sessione client / server sono i seguenti:

- **Session ID:** identifica la sessione univocamente tra tutte quelle attive all'interno del server
- **Certificate:** certificato X.509v3 dell'altrà entità coinvolta
- **Compression Method:** indica la compressione eventualmente utilizzata per comprimere e decomprimere i dati trasportati dal protocollo SSL/TLS
- **Chiper Spec:** specifica l'algoritmo simmetrico utilizzato per la codifica dei dati e la funzione di digest utilizzata per calcolare la segnatura dei messaggi

- **Master Secret:** rappresenta un segreto a 48 byte condiviso tra client e server
- **Resumable:** indica se la stessa sessione può essere utilizzata per gestire nuove connessioni.

Lo scopo della fase iniziale di **Handshake** è consentire alle due entità coinvolte di condividere un comune **master secret** per ogni nuova sessione SSL/TLS; per ogni connessione attiva è necessario definire quattro diverse chiavi:

- **server MAC secrec:** chiave utilizzata dal server per produrre la segnatura dei messaggi trasmessi
- **client MAC secret:** chiave utilizzata dal client per produrre la segnatura dei messaggi trasmessi
- **server write key:** chiave utilizzata dal server per cifrare tutti i dati trasmessi
- **client write key:** chiave utilizzata dal client per cifrare tutti i dati trasmessi.

Per ogni connessione attiva le entità coinvolte mantengono anche i seguenti parametri:

- **server random number:** numero casuale generato dal server scambiato durante la fase iniziale di handshake
- **client random number:** numero casuale generato dal client scambiato durante la fase iniziale di handshake
- **IV:** stabilisce il vettore di inizializzazione necessario per codificare i dati in accordo ad uno schema CBC (Cipher Block Chaining)
- **sequence number:** indica la posizione dei messaggi trasmessi e ricevuti da ogni entità all'interno del flusso dati.

Il protocollo **TLS Record** rappresenta la componente SSL/TLS responsabile del servizio di trasferimento dati vero e proprio; questo protocollo provvede alla frammentazione, compressione, segnatura e codifica di tutti i messaggi SSL.

Il protocollo **Alert** è responsabile di allertare le entità di eventuali malfunzionamenti.

Il protocollo **Change Cipher Spec** è la componente del protocollo responsabile di regolare ogni modifica dei parametri associati ad una sessione SSL/TLS.

Il protocollo **TLS Handshake** rappresenta la componente responsabile della negoziazione iniziale.