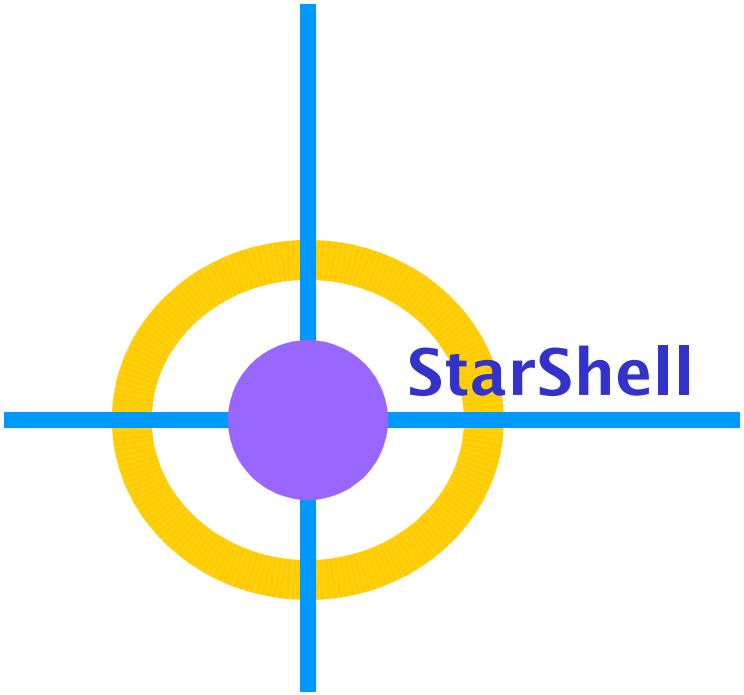
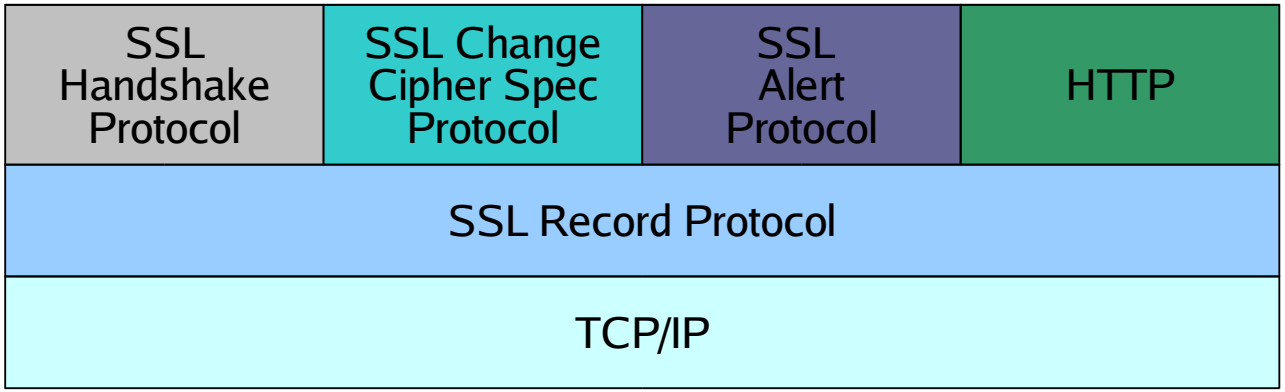


Ssl/Tls

Secure Socket Layer

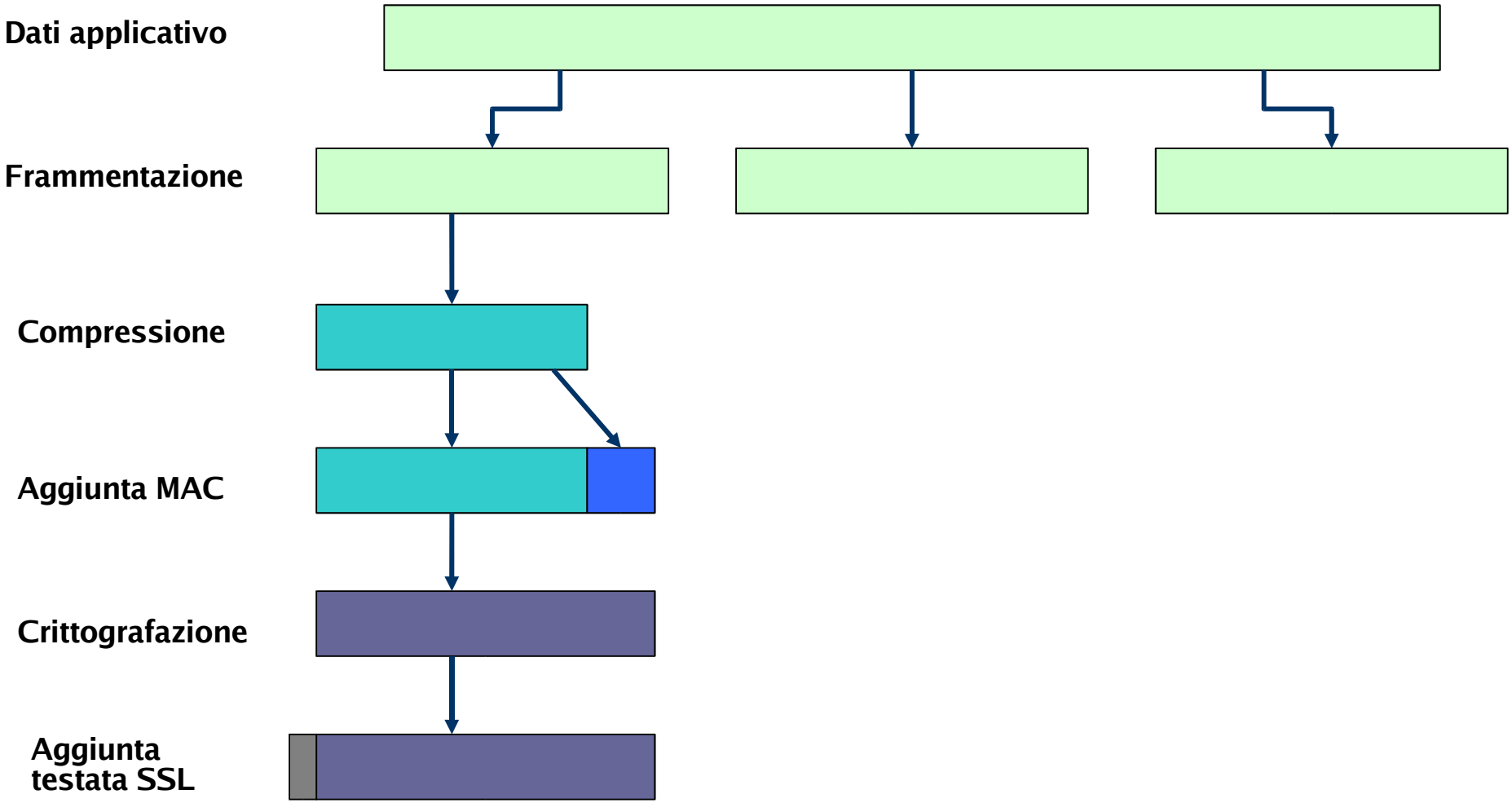
- SSL 3.0
  - **Originato da Netscape, ora pubblico**
- Autenticazione del Server con certificato
- Canale di comunicazione crittografato
  - **Chiavi doppie per la negoziazione**
  - **Chiave singola per la sessione**
- Garantisce l'integrità dei dati
- Deve essere supportato dal Server e dal Browser



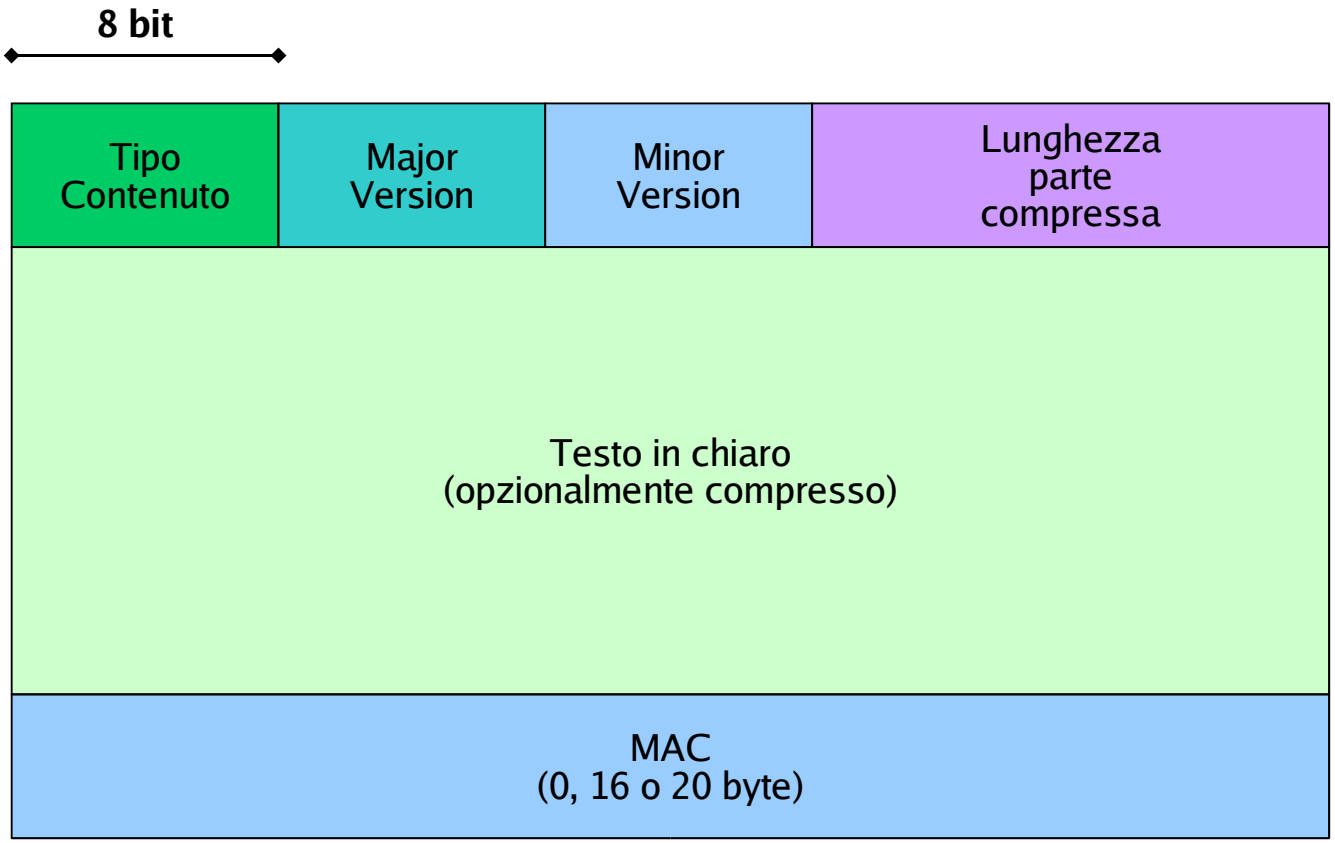
Secure Socket Layer

- Protocollo trasparente agli applicativi
  - livello di Sessione e Presentazione
- Supporta solo TCP
  - non supporta SNMP, NFS, DNS
  - Porti assgnati da IANA:
    - **HTTPS: 443**
    - **SSMTP: 465**
    - **SSNTP: 563**
    - **SSL-LDAP: 636**
    - **SPOP3: 995**
  - Altri porti non ufficiali per FTP, IMAP, Telnet, IRCS

Operazione del Protocollo SSL

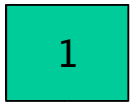


Formato Record SSL



Protocolli di Servizio SSL

Change Cipher Spec Protocol



Singolo byte settato a 1
Copia lo stato temporaneo allo stato corrente e update dello schema di cifratura.

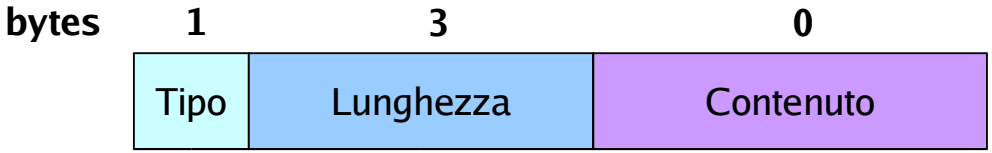
Alert Protocol

Tipi di allerta

- unexpected message
- bad_record_mac
- decompression_failure
- handshake_failure
- illegal_parameter
- close_notify
- no_certificate
- bad_certificate
- unsupported_certificate
- certificate_revoked
- certificate_expired
- certificate_unknown

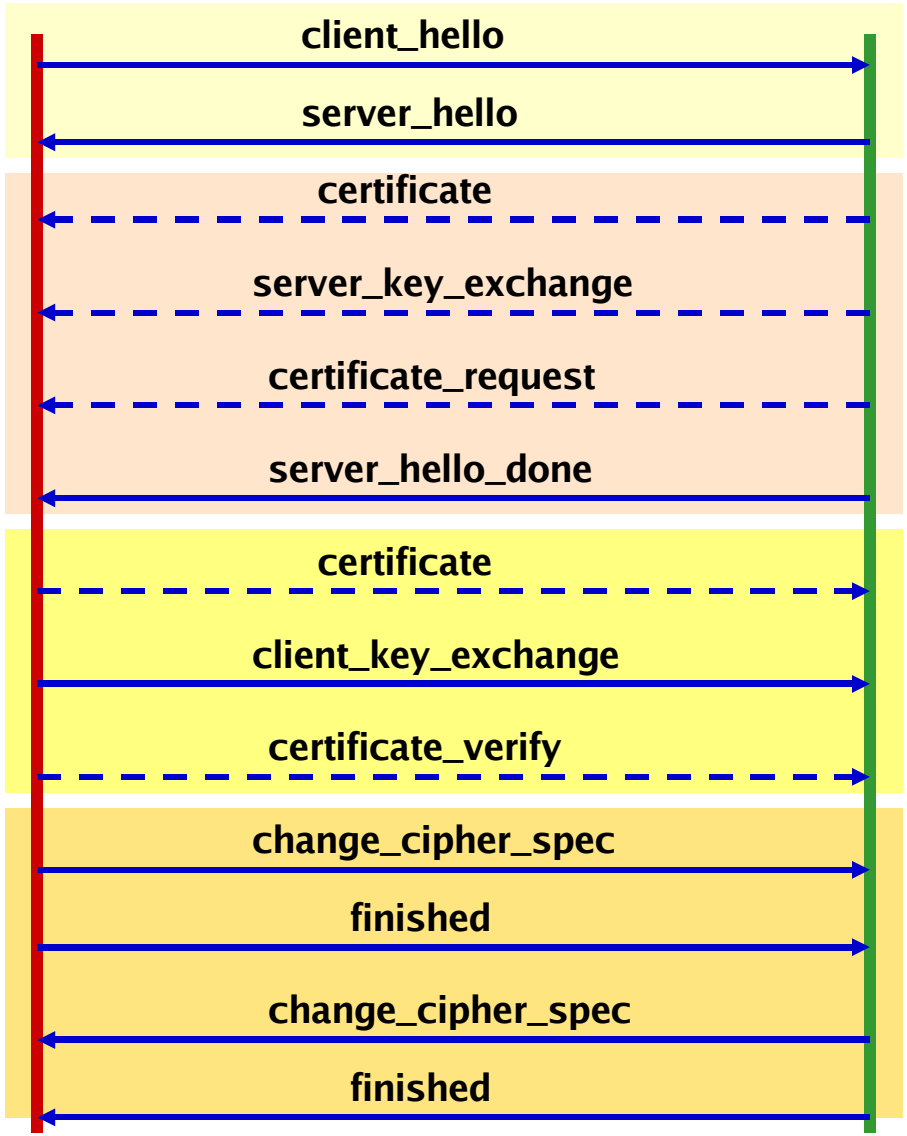
Protocolli di Servizio SSL

Protocollo di Handshake



Tipo Messaggio	Parametri
hello_request	-
client_hello	versione, casuale, id sessione, dettaglio cifra, metodo compressione
server_hello	versione, casuale, id sessione, dettaglio cifra, metodo compressione
certificate	catena di certificati X.509
server_key_exchange	parametri, firma
certificate_request	tipo, autorità
server_done	-
certificate_verify	firma
client_key_exchange	parametri, firma
finished	valore di hash

Fasi di Handshake



Dettagli Cifra SSL

- Metodo di scambio chiavi
  - RSA
  - Diffie-Hellman fisso
  - Diffie-Hellman effimero
  - Diffie-Hellman anonimo
  - Fortezza

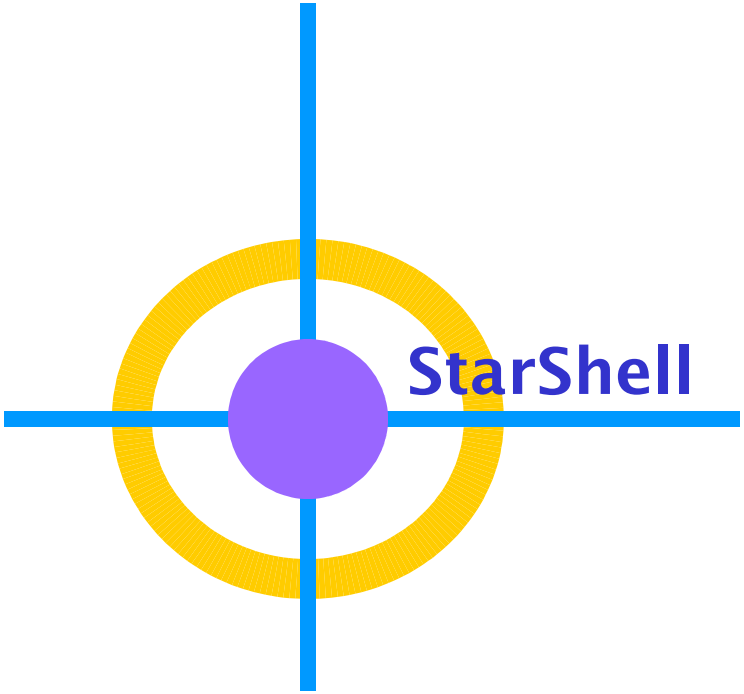
    - **Influenza il materiale che sarà contenuto nel successivo messaggio Server_Key_Exchange**

Dettagli Cifra SSL

- Algoritmo di cifra
  - **RC4, RC2, DES, 3DES, DES40, IDEA, Fortezza**
- Algoritmo MAC
  - **MD5, SHA-1**
- Tipo cifra
  - **Stream o Blocchi**
- E' esportabile
  - **vero o falso**
- Dimensione hash
  - **0, 16 (MD5) o 20 (SHA-1) bytes**
- Materiale di generazione chiave
- Dimensione del vettore di inizializzazione per CBC

Transport Layer Security (TLS)

- Standard IETF molto simile a SSL. Maggiori differenze:
  - **Due nuovi schemi di MAC**
  - **Funzione pseudocasuale per espandere le chiavi segrete in blocchi di dati**
    - **contromisura agli attacchi alle segnature di hash**
  - **Codici di allerta aggiuntivi**
  - **Non supporta Fortezza**
  - **Più tipi di certificati**
  - **Metodo di calcolo degli hash è leggermente diverso**
  - **Maggiore efficienza dei calcoli crittografici**
  - **Possibilità di padding variabile dei dati**
    - **contromisura ad analisi del traffico**


StarShell