

Tipo di messaggio	Parametri
hello_request	null
client_hello	versione, random, session id, suite di cifratura, metodo di compressione
server_hello	versione, random, session id, suite di cifratura, metodo di compressione
certificate	catena di certificati X.509v3
server_key_exchange	parametri, firma
certificate_request	tipo, authorities
server_done	null
certificate_verify	firma
client_key_exchange	parametri, firma
finished	valore hash