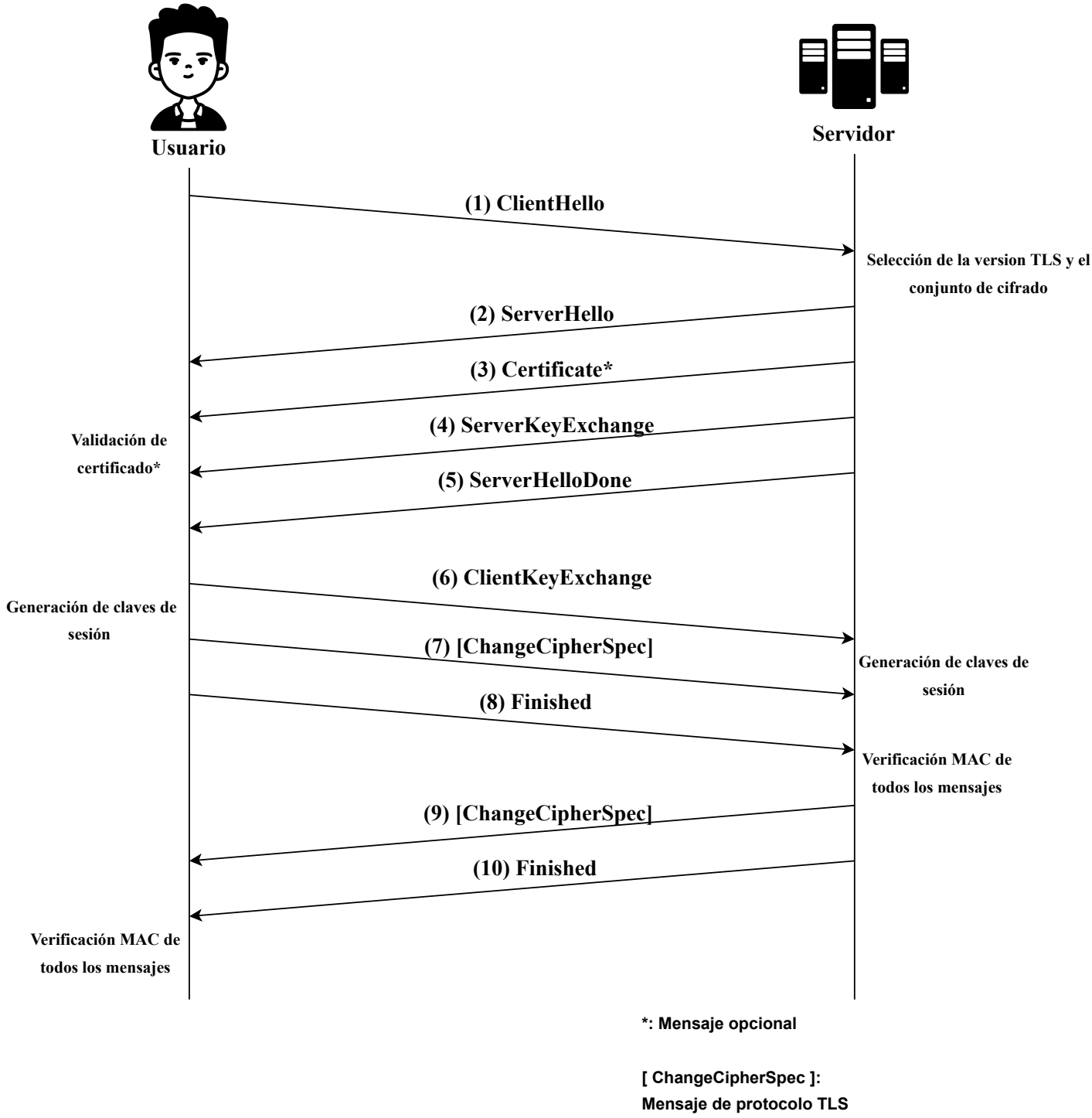
Usuario
Servidor
(1) ClientHello
Selección de la version TLS y el conjunto de cifrado
(2) ServerHello
(3) Certificate*
(4) ServerKeyExchange
Validación de certificado*
(5) ServerHelloDone
(6) ClientKeyExchange
Generación de claves de sesión
(7) [ChangeCipherSpec]
Generación de claves de sesión
(8) Finished
Verificación MAC de todos los mensajes
(9) [ChangeCipherSpec]
(10) Finished
Verificación MAC de todos los mensajes
*: Mensaje opcional
[ChangeCipherSpec]:
Mensaje de protocolo TLS