



**Turma:** RSI 1º B

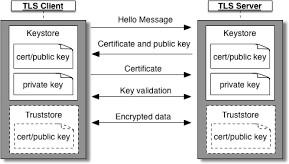
**Nº:** 30156

**Nome:** Pedro Rodrigues

# Negociação entre cliente e servidor

O SSL e TLS são protocolos de criptografia para internet, permitem a comunicação segura entre o cliente e o servidor através de uma aplicação web. O cliente e o servidor ao usar uma ligação, utilizando um procedimento de handshaking para o qual o cliente e o servidor concordam em vários parâmetros para estabelecer uma ligação segura. Funciona na seguinte forma:

* O cliente envia ao servidor a sua a versão que possui do TSL/SSL, as definições de criptografia, os dados da sessão e as informações que o servidor precisa para comunicar com o cliente.
* O servidor envia ao cliente a sua versão do TSL/SSL, as configurações de criptografia, os dados da sessão e as informações que o cliente precisa.
* O cliente utiliza as informações disponibilizadas pelo servidor para se autenticar ao servidor o para confirmar se todas as definições recebidas pelo servidor se são esperadas para fazer a comunicação segura.
* Utilizando os dados gerados no handshaking, o cliente cria a sua chave privada para a sessão e, em seguida envia a chave encriptada para o servidor
* O cliente envia uma mensagem para o servidor, informado que as próximas mensagens serão encriptadas com a chave privada criada na sessão, de seguida envia uma mensagem encriptada, indicando que o handshanking do cliente está concluído.
* O servidor envia uma mensagem para o cliente informando que as próximas mensagens serão encriptadas com a chave privad de sessão e envia uma mensagem encriptada indicado que o handshanking do servidor está concluído.



# Chave e encriptação SSL/TLS

Para autentificação do servidor: O cliente utiliza a chave publica do servidor do servidor para encriptar os dados são utilizados para criar uma chave privada. O servidor poderá gerar a chave privada se puder desencriptar os dados com a chave privada certa.

Para autentificação do cliente: o servidor utiliza a chave publica do certificado do cliente para desencriptar os dados enviados pelo cliente.

A troca de mensagens concluídas que são encriptadas com a chave privada que confirma a autentificação está concluída e é utilizado o algoritmo RSA para este método de encriptação.