**Apache Tomcat SSL Configuration**

Secure Socket Layer (SSL) is a protocol that provides security for communications between client and server by implementing encrypted data and certificate-based authentication. Technically, the term "SSL" now refers to the Transport Layer ouSecurity (TLS) protocol, which is based on the original SSL specification.

SSL is one of the most common ways of integrating secure communication on the internet, as it is a mature protocol that is well-supported by every major browser and a number of well-respected organizations provide third party SSL authentication services.

The SSL protocol aims to provide solutions to two simple security problems:

1. How can we securely transmit data between two parties in such a way that only the two parties can read it?
2. How can one (or more) of the parties involved prove that they are actually the entity we want to grant the ability to decrypt our encrypted transmission?

### HTTPS vs. HTTP

The most common way that SSL is integrated into Internet communications is through the HTTPS protocol. Calling HTTPS a "protocol" is not entirely accurate, as it is simply a combination of the HTTP and SSL protocols. When we say a message was sent using HTTPS, what we are actually saying is that the message was first encrypted using SSL, transmitted and received using normal HTTP protocol, and then decrypted by the receiver, also with SSL.

**Short Summary:**

* SSL offers security through encryption
* the encryption process is made possible through the use of digital certificates verified by a third party Certificate Authority
* The most common implementation of this process is the HTTPS combination protocol.