RAKSHA.IO

At Raksha.io we develop applications for web security environments. This includes the basics of PKI and that is X.509 authentications.

The most common use of X.509 certificate authentication is in verifying the identity of a server when using SSL/TLS 2.0, most commonly when using HTTPS from a browser. The browser will automatically check that the certificate presented by a server has been issued (ie digitally signed) by one of a list of trusted certificate authorities which it maintains.

Using TLS / SSL with “mutual authentication”; the server will then request a valid certificate from the client as part of the SSL handshake. The server will authenticate the client by checking that its certificate is signed by an acceptable authority. If a valid certificate has been provided, it can be obtained through the callbacks in an application. Raksh.io Security X.509 module extracts the certificate using a filter. It maps the certificate to an application user and loads that user's set of granted authorities for use with the standard Spring Security infrastructure.