X509 Sertifika Tabanlı Kimliklendirme

X509 ve HTTPS

- Sertifika tabanlı kimliklendirme için **HTTPS** gereklidir
- HTTPS de **iki yönlü kimliklendirme** yapılır
  - Server authentication
  - Client authentication
- Sunucu tarafı kimliklendirmesi **zorunlu**dur
- Tarayıcı sunucunun gönderdiği sertifikayı kendi “**trusted certificate authorities**” ile doğrulamaya çalışır

X509 ve HTTPS

- İstemci kimliklendirmesi ise **opsiyonel**dir
- Aktive edildiği vakit sunucu, **SSL handshake sırasında** istemciden sertifika talep eder
- Bu sertifikayı kendi "**trusted certificate authorities**" ile doğrulamaya çalışır
- Daha sonra bu sertifika **Servlet API** üzerinden uygulama tarafında erişilebilir
  - `httpServletRequest.getAttribute("javax.servlet.request.X509Certificate");`

Tomcat SSL Konfigürasyonu

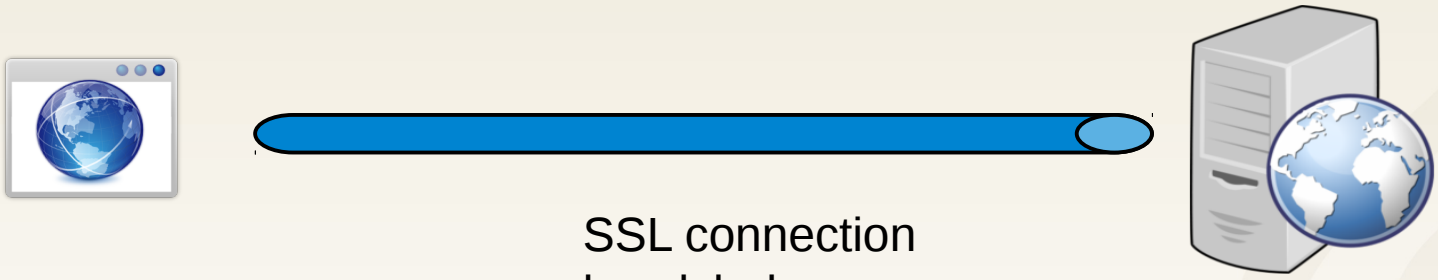
```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" scheme="https"
secure="true"
           clientAuth="true" sslProtocol="TLS"
           keystoreFile="${catalina.home}/conf/server.jks"
           keystoreType="JKS" keystorePass="changeit"
           truststoreFile="${catalina.home}/conf/server.jks"
           truststoreType="JKS" truststorePass="changeit"/>
```

- Tomcat'in **server.xml**'inde yukarıdaki ayarlar yapılmalıdır
- Default olarak **tomcat keystore**'da tomcat alias'ı (**tomcat**) ile bir sertifika aramaktadır
- Keystore şifresini de default olarak "**changeit**" olarak kabul etmektedir

Tomcat SSL Konfigürasyonu

- İstemci geçerli bir sertifika göndermediği takdirde **HTTPS bağlantısı kurulamayacak**tır
- **clientAuth=”want”** şeklinde tanımlanırsa istemci geçerli sertifika göndermese de HTTPS bağlantısının kurulması sağlanabilir
- Böyle bir konfigürasyonda kullanıcıya **alternatif olarak** form tabanlı bir kimliklendirme opsiyonu da sunmak gerekebilir

Tomcat SSL Konfigürasyonu



Client authentication opsiyoneldir. tarayıcı üzerinden user sertifikası sunucuya iletilir. Sunucu bu sertifikayı trusted CA'ler ile doğrulamaya çalışır. Sertifika doğrulanırsa SSL bağlantısı kurulabilir.

Tomcat'de truststoreFile ile belirtilen keystore'da trusted CA'ler bulunur. Tomcat istemciden gelen user cert'i bunlarla validate etmeye çalışır.

Server authentication zorunludur. Server keystore'dan alınan sunucu sertifikası istemciye gönderilir. istemci(tarayıcı) bu sertifikayı trusted CA'ler ile doğrulamaya çalışır. Sertifika doğrulanırsa SSL bağlantısı kurulabilir.

Tomcat'de keystoreFile ile belirtilen keystore'dan sunucu sertifikası elde edilir.

X509 Kimliklendirme Konfigürasyonu

- `<security:http>` elemanı içerisinde `<security:x509>` elemanı ile gerçekleştirilir

```
<security:http>
    <security:x509 subject-principal-regex="CN=(.*)"
user-service-ref="userService"/>
</security:http>
```

- Yukarıdaki konfigürasyonda **common name field**'ındaki değer **username** olarak alınır
- Örneğin, emailAddress=(.*) gibi bir ifade de ise e-mail adresi username olacaktır

X509 Kimliklendirme Konfigürasyonu

- Spring Security X509 sertifikasını request'den almak için bir **filter** kullanır
- Sertifikayı request'den aldıktan sonra username'i **extract** eder
- Ardından **UserDetailsService** bean'ini kullanarak **Authentication** nesnesini populate eder
- Eğer request'de geçerli bir sertifika bulunamaz ise veya username elde edilemez ise **SecurityContext** boş bırakılır

İletişim

- Harezmi Bilişim Çözümleri
- Kurumsal Java Eğitimleri
- http://www.java-egitimleri.com
- info@java-egitimleri.com