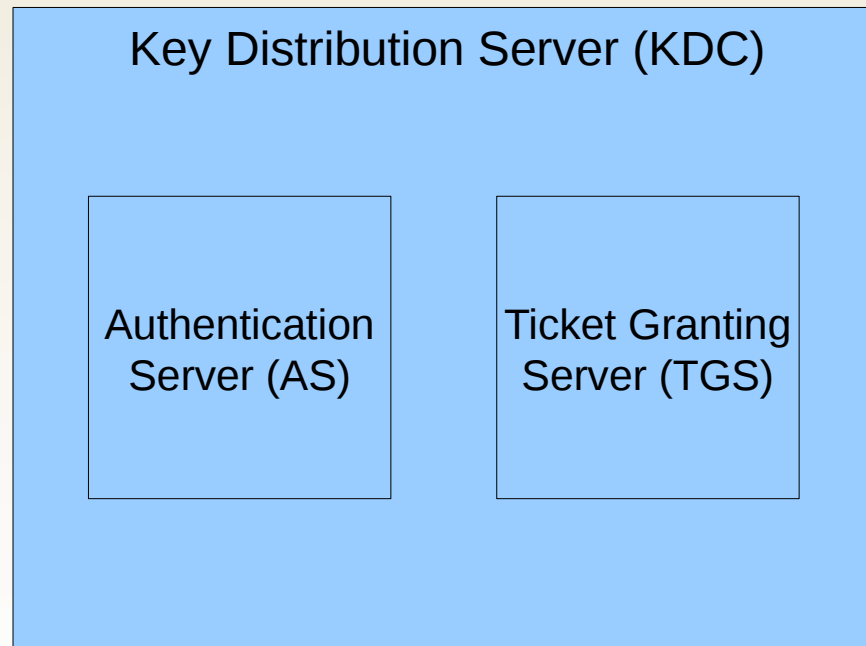


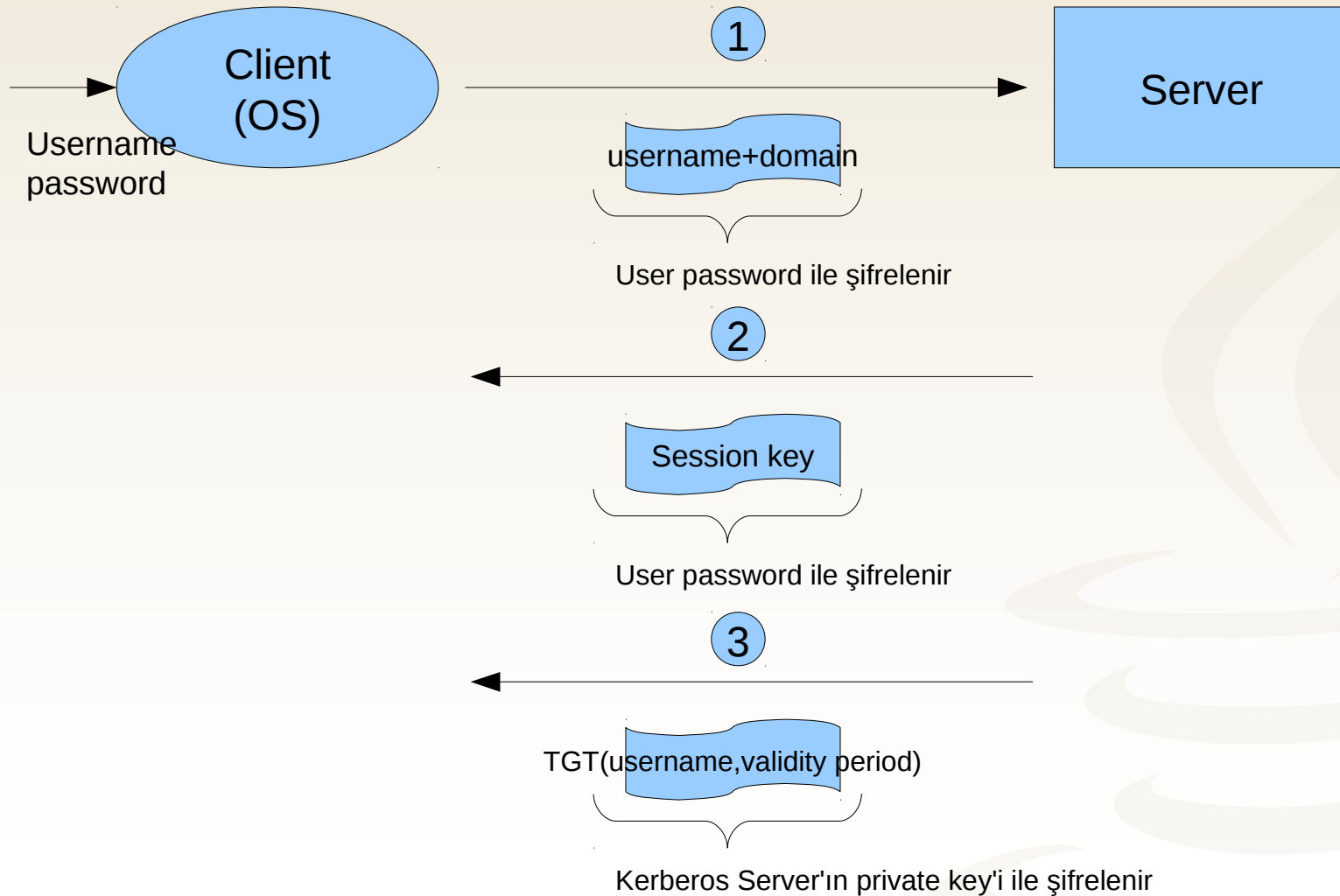
Spring Security ve Kerberos Auth



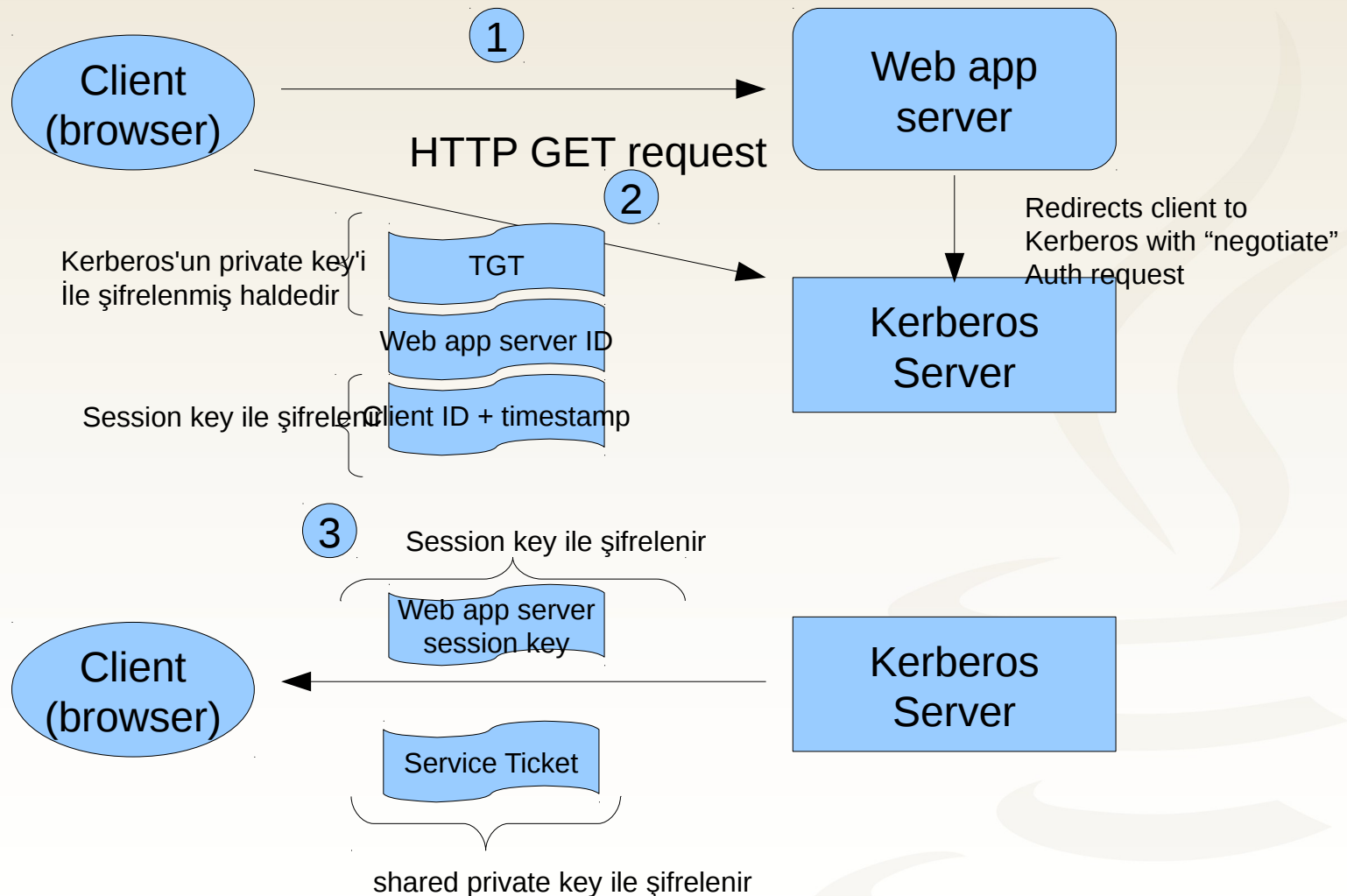
Kerberos Server'in Yapısı



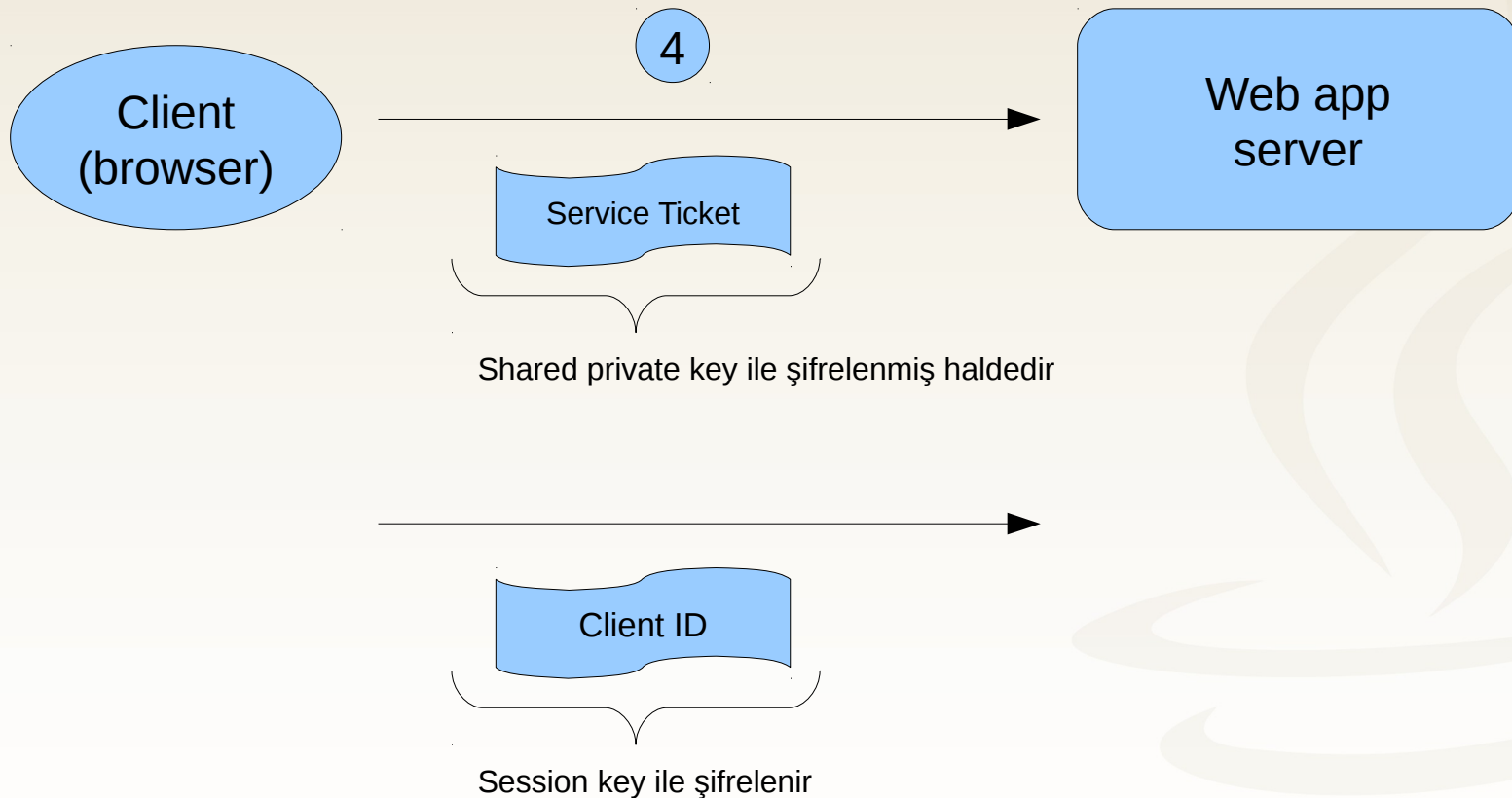
Kerberos Initial Authentication



Kerberos Web App Authentication



Kerberos Web App Authentication



Windows Active Directory & Kerberos

- Win 2000 sonrası kimliklendirme kerberos ile yapılmaktadır
- Domain Controller kerberos authentication'ı gerçekleştirmektedir
- Active directory aynı zamanda bir KDC'dir

Kerberos Web App Authentication

- Web uygulamasının öncelikle kerberos server'a tanıtılması gerekir
 - Principal ID
 - Shared secret private key elde edilir
- Örnek Principal ID:
`HTTP/webapp.harezmi.com.tr/HAREZMI.COM.TR`
- Bu bilgilerin elde edilme şekli kerberos impl. arası farklılık gösterebilir

Win 2008 AD Server'da İşlemler

- “Service principal” olacak şekilde bir user tanımı yapılır
 - User'a **SPN assignment**'ı yapılır
([HTTP/webapp.harezmi.com.tr/HAREZMI.COM.TR](http://webapp.harezmi.com.tr/HAREZMI.COM.TR))
- **Deactivate** "User must change password at next logon"
- **Activate** "Password never expires"

Win 2008 AD Server'da İşlemler

- **ktpass.exe** ile shared private key elde edilir
 - `ktpass /out http-web.keytab /mapuser http-webapp.harezmi.com.tr@HAREZMI.COM.TR /princ HTTP/webapp.harezmi.com.tr@HAREZMI.COM.TR /pass *`

Spring Security ve Kerberos

- **SpnegoEntryPoint** ve **SpnegoAuthenticationProcessingFilter** “handshake” den sorumludur
- **KerberosServiceAuthenticationProvider** ise “service ticket”ı validate eder
- Kerberos sadece “username” döner
- Diğer user attribute ve rol bilgileri ise **userDetailsService** ile elde edilir

Firefox ve Negotiate Auth

- Default olarak disabled durumdadır
- About:config ile konfigürasyon bilgileri listelenir
- **network.negotiate-auth.trusted-uris** parametresinin değeri domain name ile değiştirilir

İletişim

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

