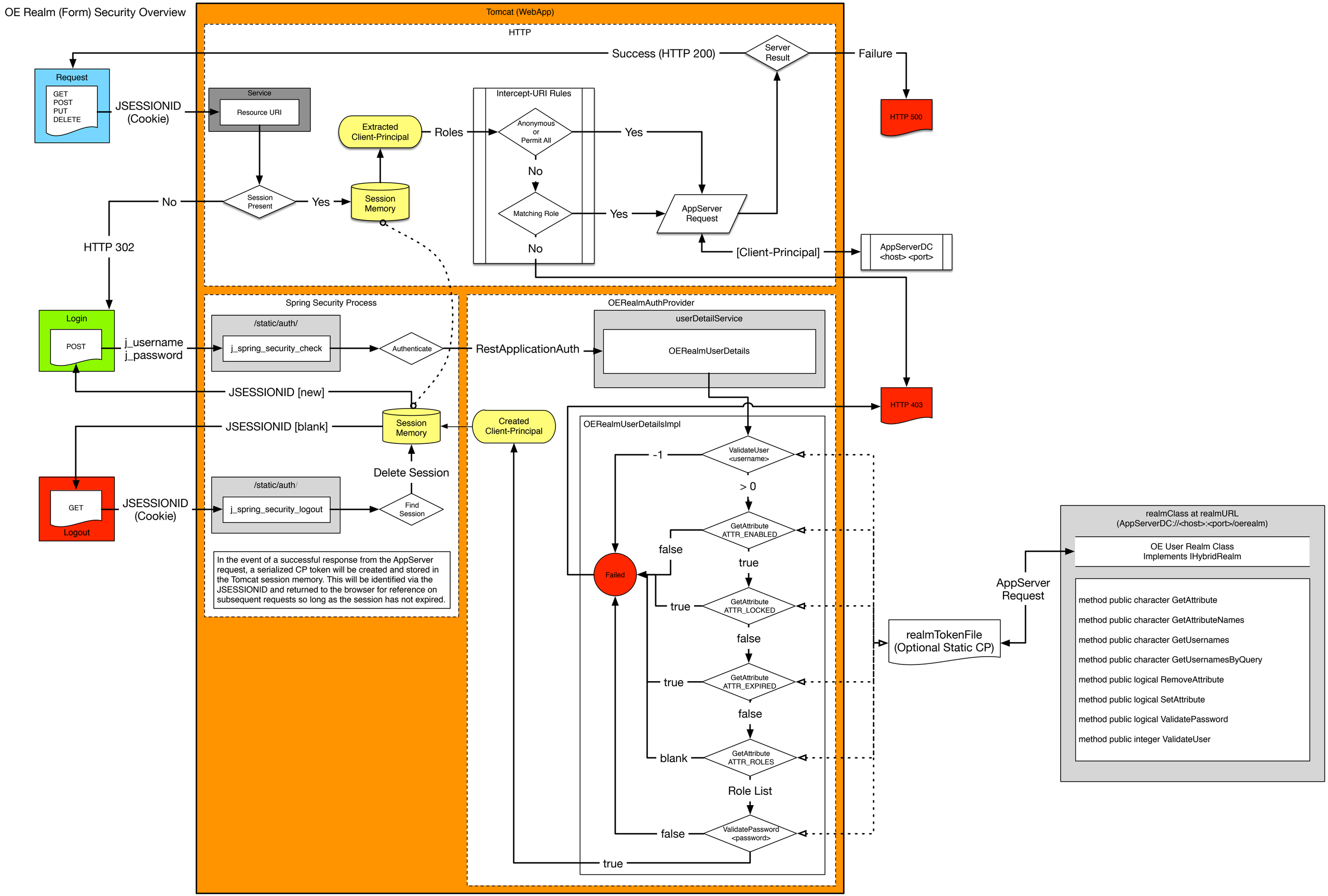
OE Realm (Form) Security Overview
Tomcat (WebApp)
HTTP
Success (HTTP 200)
Server Result
Failure
HTTP 500
Request
GET
POST
PUT
DELETE
JSESSIONID (Cookie)
Service
Resource URI
Extracted Client-Principal
Roles
Intercept-URI Rules
Anonymous or Permit All
Yes
No
Matching Role
Yes
No
AppServer Request
[Client-Principal]
AppServerDC <host> <port>
Session Present
No
Yes
Session Memory
HTTP 302
Spring Security Process
/static/auth/
j_spring_security_check
Authenticate
RestApplicationAuth
OERealmAuthProvider
userDetailService
OERealmUserDetails
Login
POST
j_username
j_password
JSESSIONID [new]
JSESSIONID [blank]
Session Memory
Created Client-Principal
HTTP 403
OERealmUserDetailsImpl
ValidateUser <username>
-1
> 0
GetAttribute ATTR_ENABLED
false
true
Failed
GetAttribute ATTR_LOCKED
true
false
GetAttribute ATTR_EXPIRED
true
false
GetAttribute ATTR_ROLES
blank
Role List
ValidatePassword <password>
false
true
Delete Session
/static/auth/
j_spring_security_logout
Find Session
GET
Logout
JSESSIONID (Cookie)
In the event of a successful response from the AppServer request, a serialized CP token will be created and stored in the Tomcat session memory. This will be identified via the JSESSIONID and returned to the browser for reference on subsequent requests so long as the session has not expired.
realmTokenFile (Optional Static CP)
AppServer Request
realmClass at realmURL (AppServerDC://<host>:<port>/oerealm)
OE User Realm Class Implements IHybridRealm
method public character GetAttribute
method public character GetAttributeNames
method public character GetUsernames
method public character GetUsernamesByQuery
method public logical RemoveAttribute
method public logical SetAttribute
method public logical ValidatePassword
method public integer ValidateUser