WCI Authentication

Interactions between tiers during authentication with servlet 2.5 API & servlet 3.0 API

Alain Defrance (eXo platform)

Two types of authentication

- Servlet 2.5 API
  - Simulation of programmatic authentication.
  - Use a set of redirect.

- Servlet 3.0 API
  - Use programmatic authentication provided by servlet 3.0 API.

Supported Servers

- Using servlet 2.5 API

  - Tomcat 6.x

  - Jetty 6.x

  - JBoss as 4.2

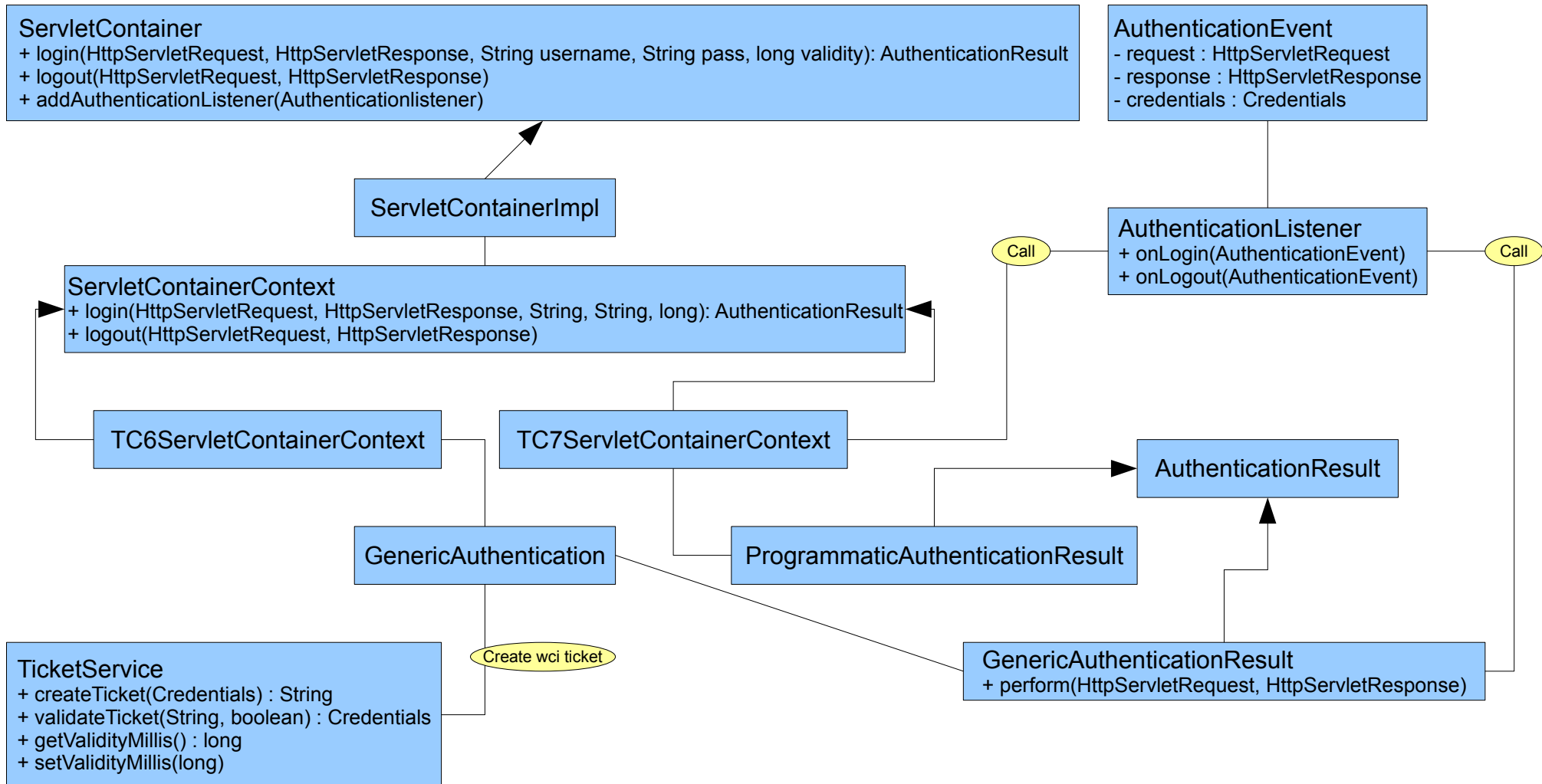 - JBoss as 5.1 (feature can't be unit tested because a bug of cargo 1.0.3)
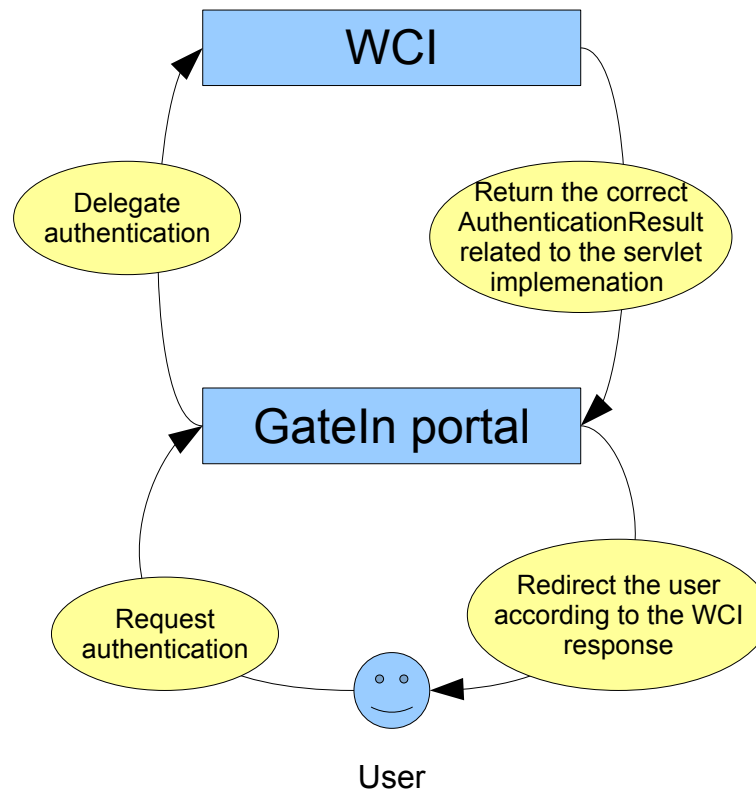
- Using servlet 3.0 API

  - Tomcat 7.x

WCI Authentication components

- Can Authenticate through JAAS

- Produce an AuthenticationResult instance

- Have authentication lifecycle listeners

- Have a JAAS LoginModule (WCILoginModule)

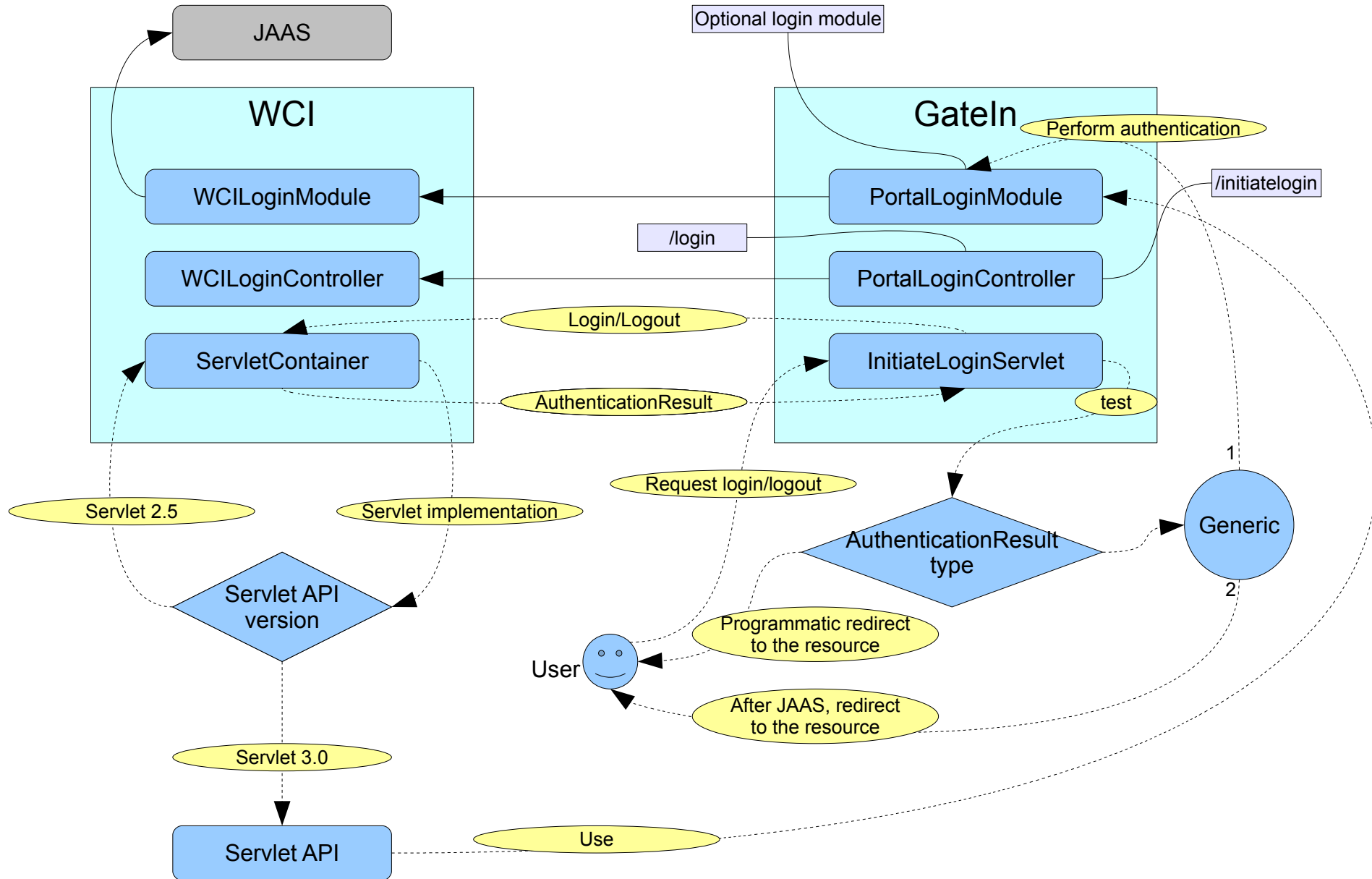- Have a Servlet (WCILoginController)

WCI Authentication API

ServletContainer
+ login(HttpServletRequest, HttpServletResponse, String username, String pass, long validity): AuthenticationResult
+ logout(HttpServletRequest, HttpServletResponse)
+ addAuthenticationListener(Authenticationlistener)

AuthenticationEvent
- request : HttpServletRequest
- response : HttpServletResponse
- credentials : Credentials

ServletContainerImpl

ServletContainerContext
+ login(HttpServletRequest, HttpServletResponse, String, String, long): AuthenticationResult
+ logout(HttpServletRequest, HttpServletResponse)

AuthenticationListener
+ onLogin(AuthenticationEvent)
+ onLogout(AuthenticationEvent)

Call

Call

TC6ServletContainerContext

TC7ServletContainerContext

AuthenticationResult

GenericAuthentication

ProgrammaticAuthenticationResult

Create wci ticket

TicketService
+ createTicket(Credentials) : String
+ validateTicket(String, boolean) : Credentials
+ getValidityMillis() : long
+ setValidityMillis(long)

GenericAuthenticationResult
+ perform(HttpServletRequest, HttpServletResponse)

WCI Authentication and GateIn

WCI

Delegate authentication

Return the correct AuthenticationResult related to the servlet implemenation

GateIn portal

Request authentication

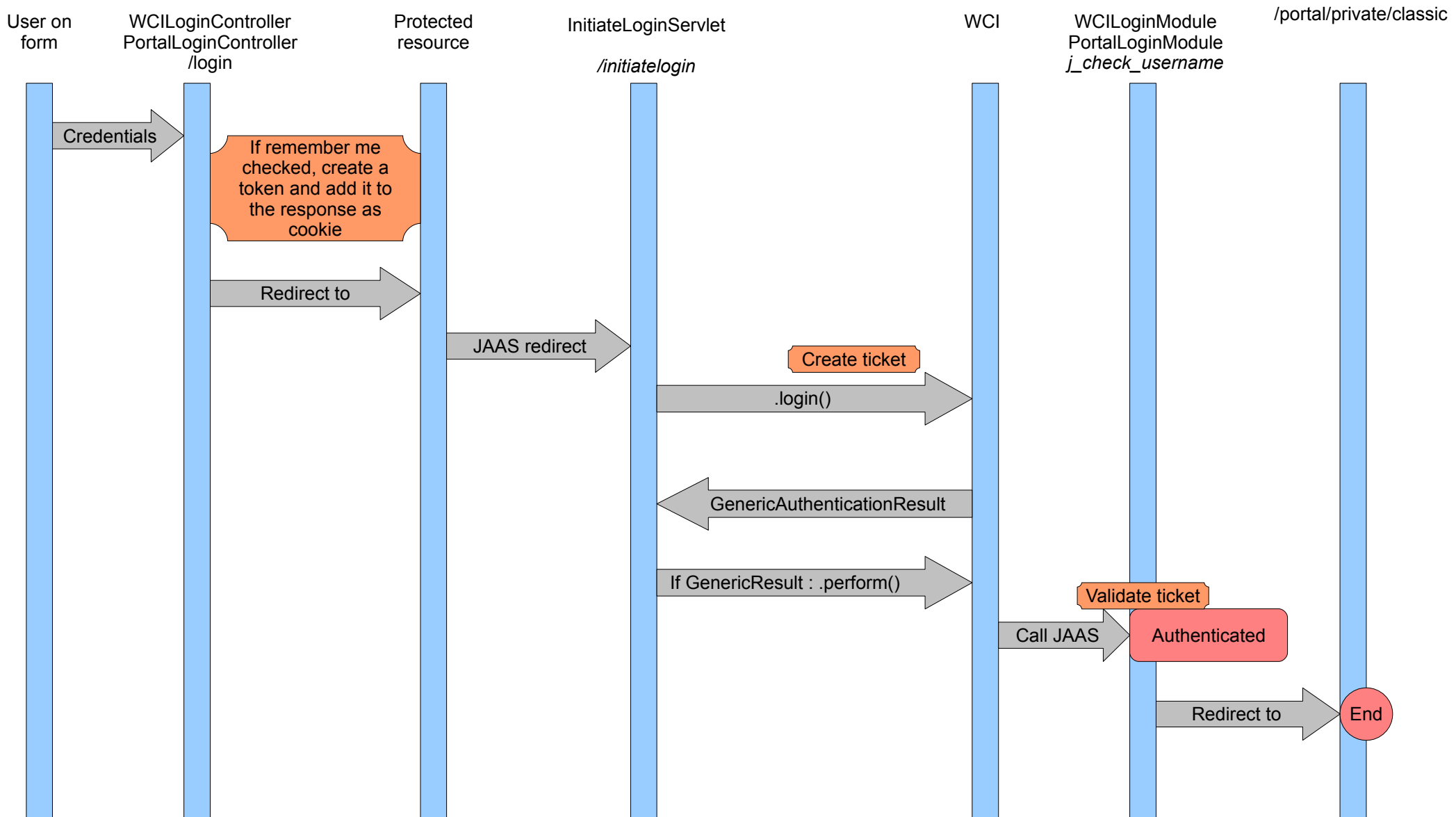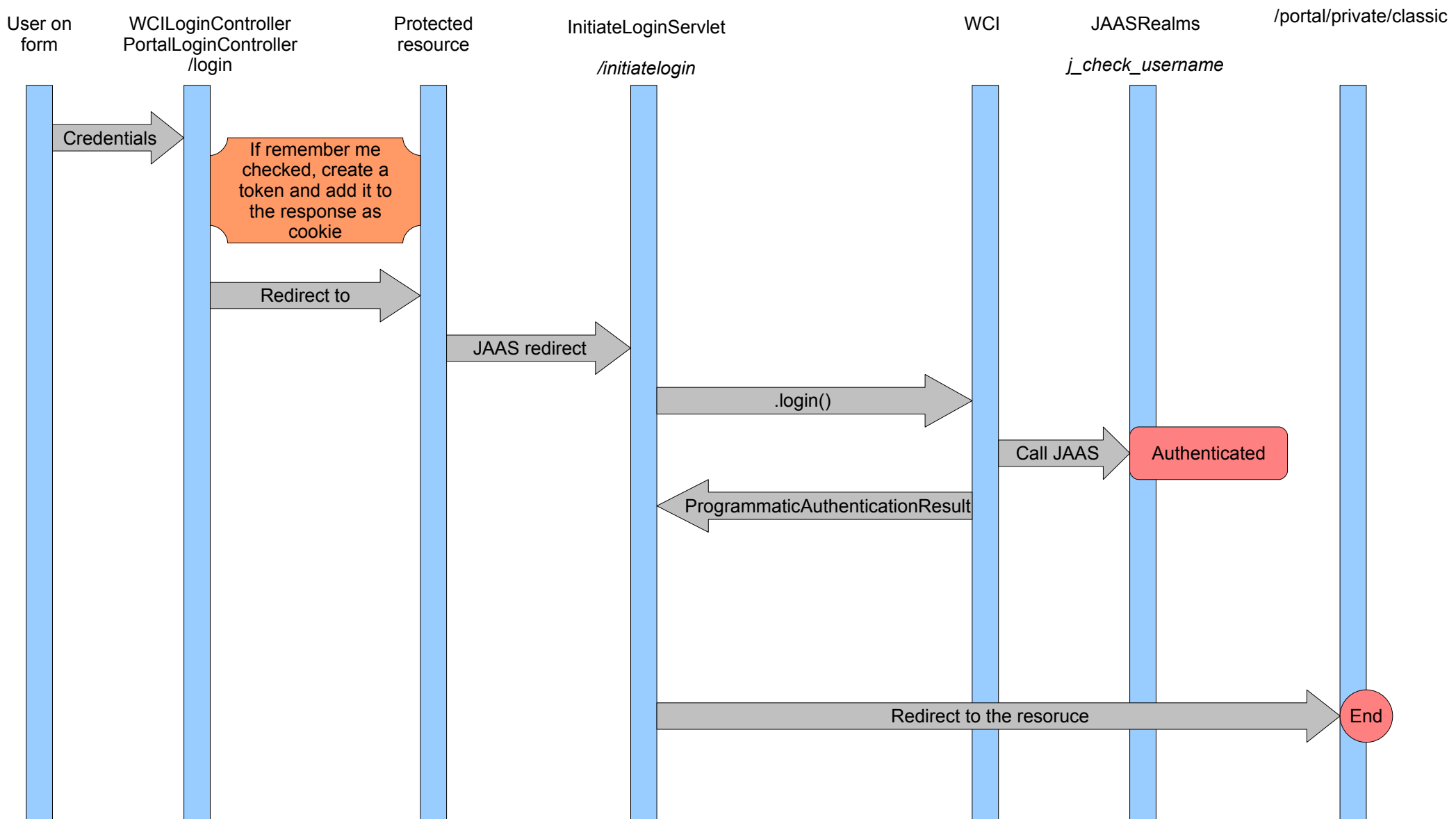Redirect the user according to the WCI response

User

GateIn Authentication

Authentication with Form

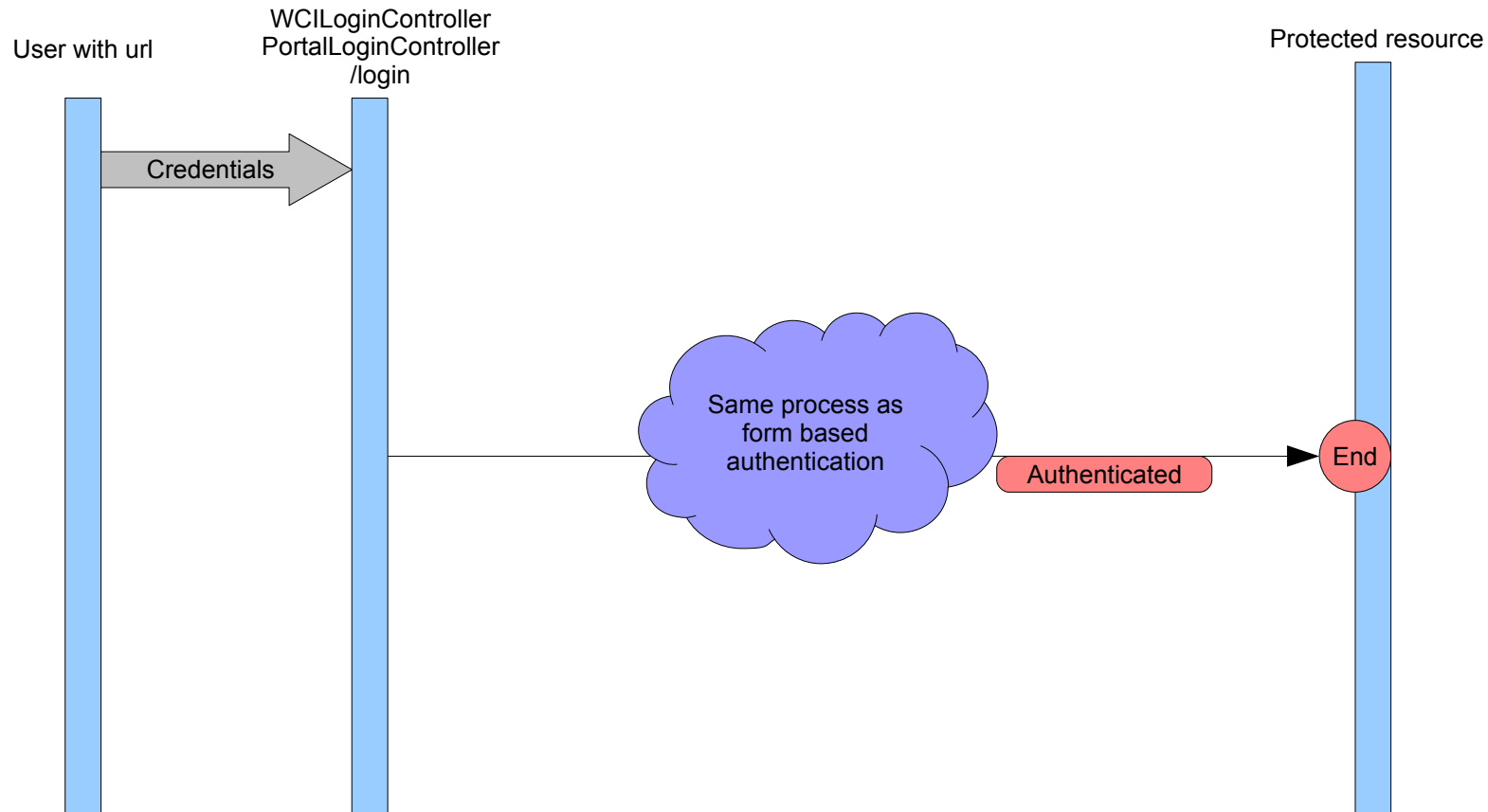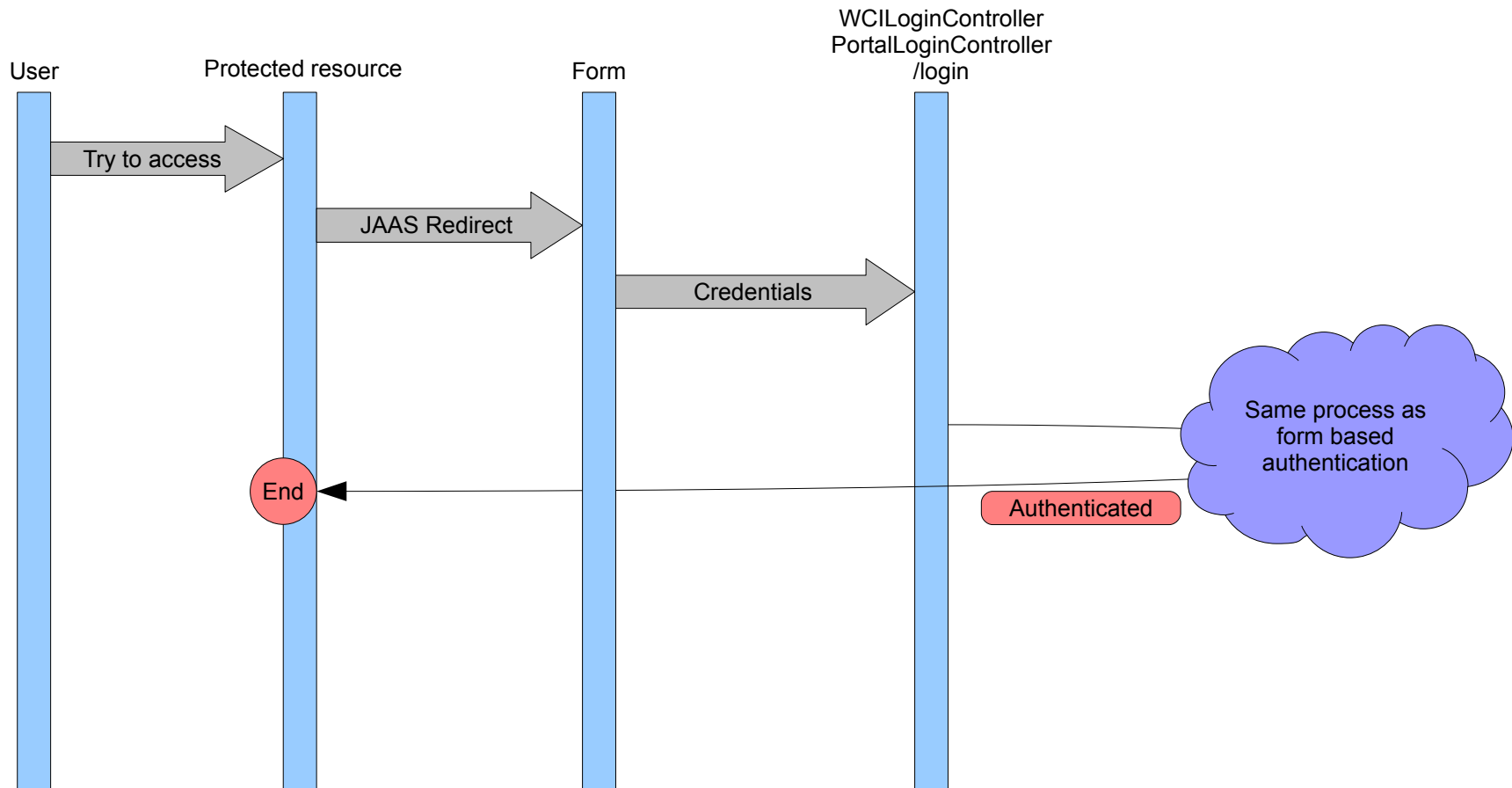This use case addresses when the end user fills in a form and submits it with a click to trigger authentication

Server 2.5

User on form

WCILoginController
PortalLoginController
/login

Protected resource

InitiateLoginServlet
/initiatelogin

WCI

WCILoginModule
PortalLoginModule
j_check_username

/portal/private/classic

Credentials

If remember me checked, create a token and add it to the response as cookie

Redirect to

JAAS redirect

Create ticket

.login()

GenericAuthenticationResult

If GenericResult : .perform()

Validate ticket

Call JAAS

Authenticated

Redirect to

End

Server 3.0

Authentication with Form

This use case addresses when the end user fills in a form and submits it with a click to trigger authentication

User on form

WCILoginController
PortalLoginController
/login

Protected resource

InitiateLoginServlet

/initiatelogin

WCI

JAASRealms

j_check_username

/portal/private/classic

Credentials

If remember me checked, create a token and add it to the response as cookie

Redirect to

JAAS redirect

.login()

Call JAAS

Authenticated

ProgrammaticAuthenticationResult

Redirect to the resoruce

End

Authentication with URL

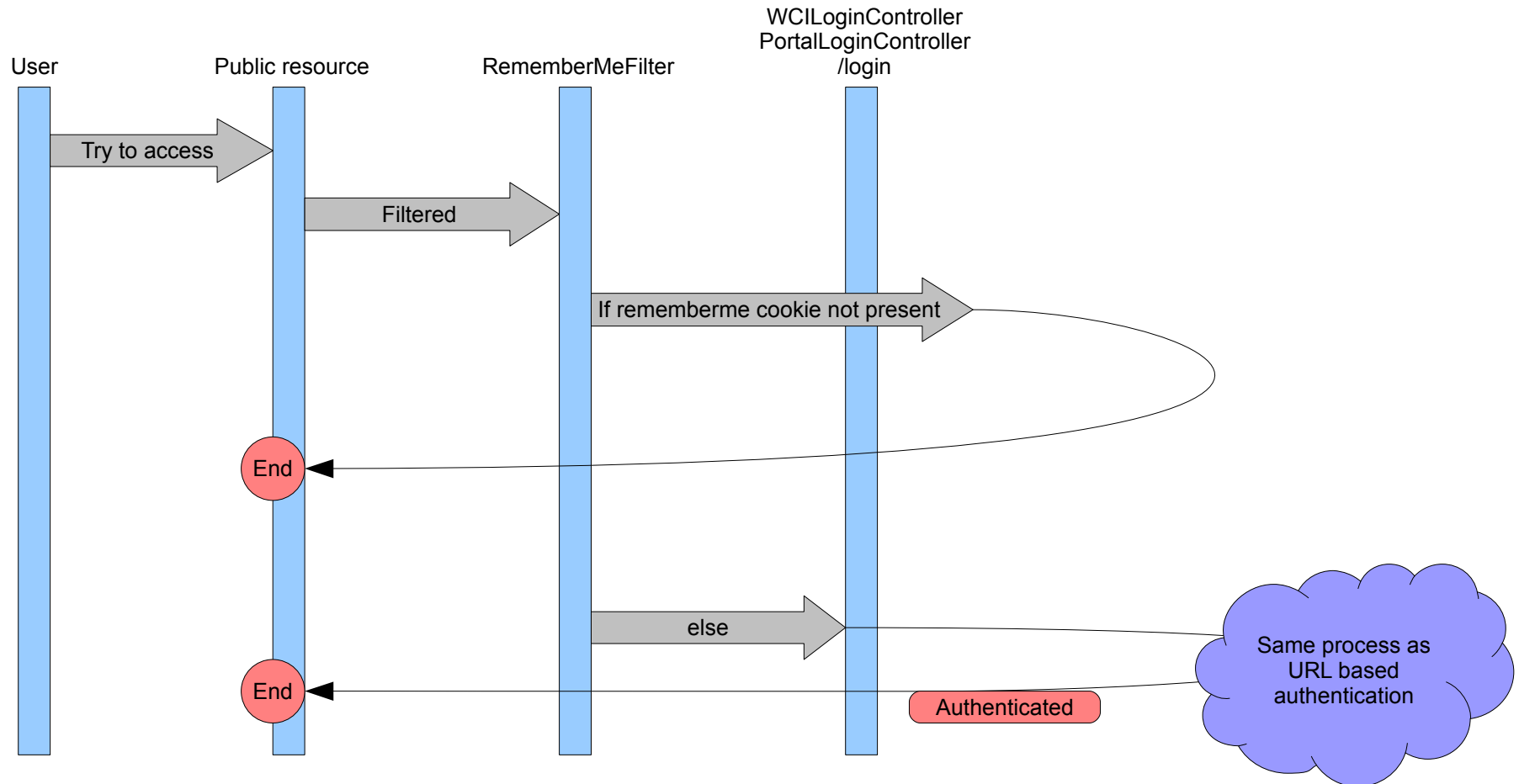This use case addresses when the end user access to an url like : /login?username=foo&password=bar

User with url

WCILoginController
PortalLoginController
/login

Protected resource

Credentials

Same process as
form based
authentication

Authenticated

End

Authentication with protected resource

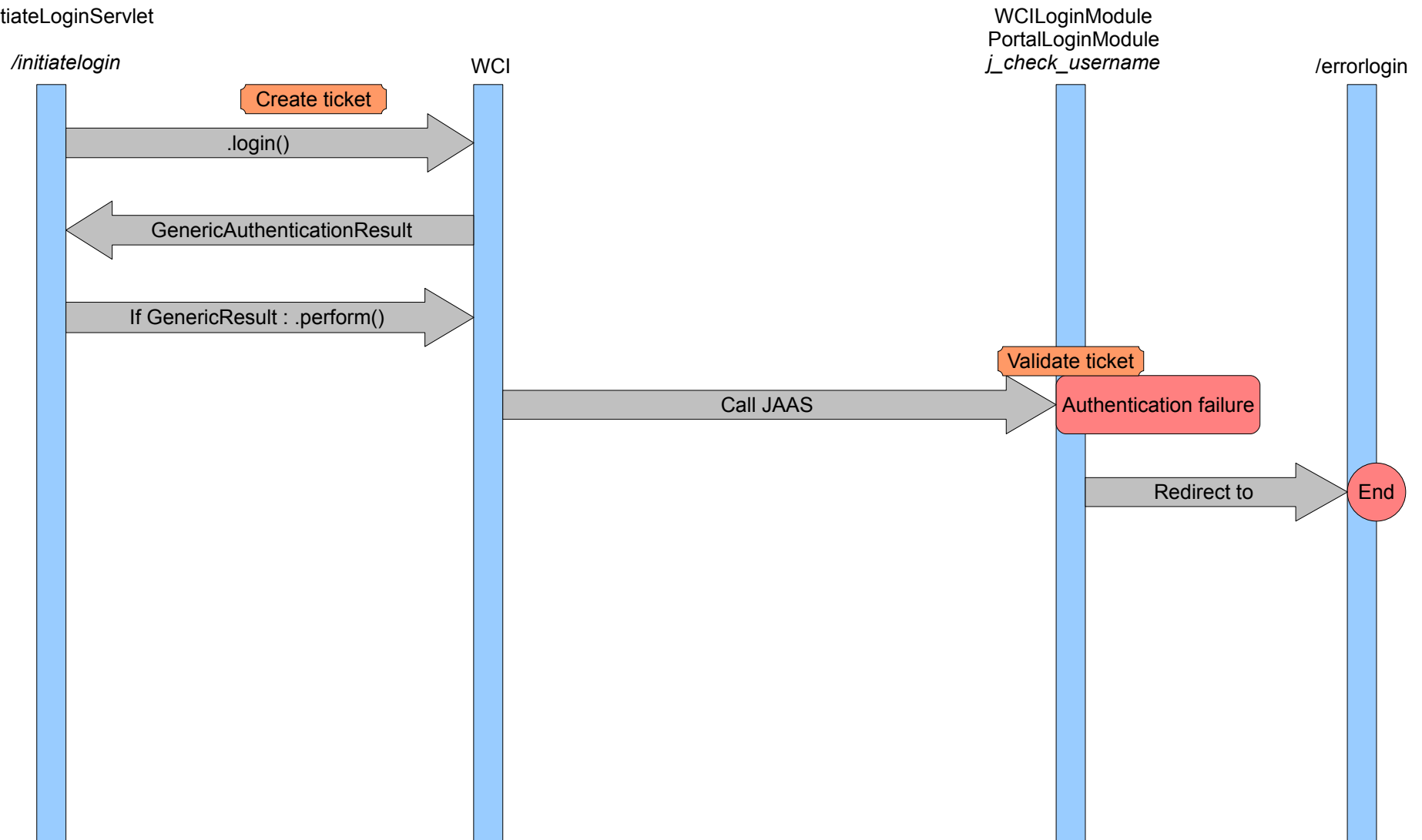This use case addresses when the end user try to access to a protected resource

User

Protected resource

Form

WCILoginController
PortalLoginController
/login

Try to access

JAAS Redirect

Credentials

Same process as
form based
authentication

End

Authenticated

Authentication with remember me cookie

This use case addresses when the end user comme to a public resource and the client have a remember me cookie

User   Public resource   RememberMeFilter

WCILoginController
PortalLoginController
/login

Try to access

Filtered

If rememberme cookie not present

End

else

End

Authenticated

Same process as
URL based
authentication

Authentication failure

Server 2.5

This use case addresses when the end user fills wrong login or password
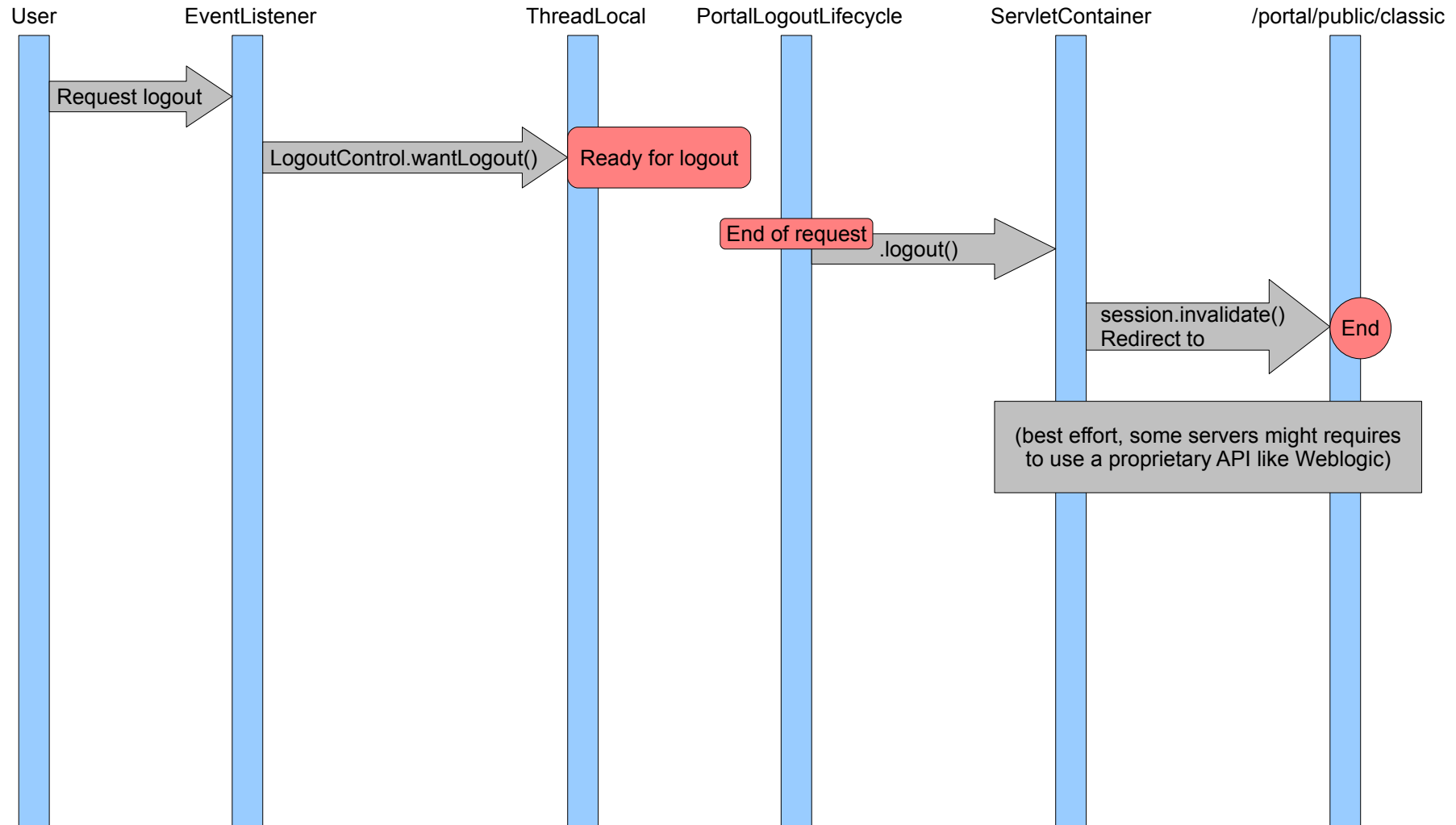
InitiateLoginServlet

/initiatelogin

WCI

WCILoginModule
PortalLoginModule
j_check_username

/errorlogin

Create ticket

.login()

GenericAuthenticationResult

If GenericResult : .perform()

Validate ticket

Call JAAS

Authentication failure

Redirect to

End