Com desenvolupar una aplicació que requereixi GICAR com a sistema d'autenticació

A qui va dirigit

Aquest how-to va dirigit a tots aquells que hagin de desenvolupar una aplicació Canigó que tingui com a requeriment estar securitzada mitjançant **GICAR**[1].

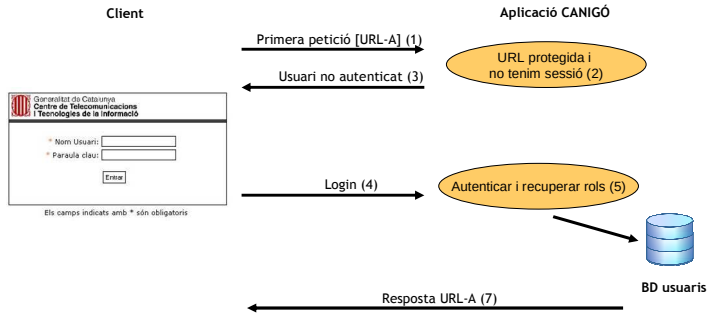
Versió de Canigó

Els passos descrits en aquest document són específics de la **versió 2.3 de Canigó**. Tot i això, poden ser d'aplicació en versions superiors.

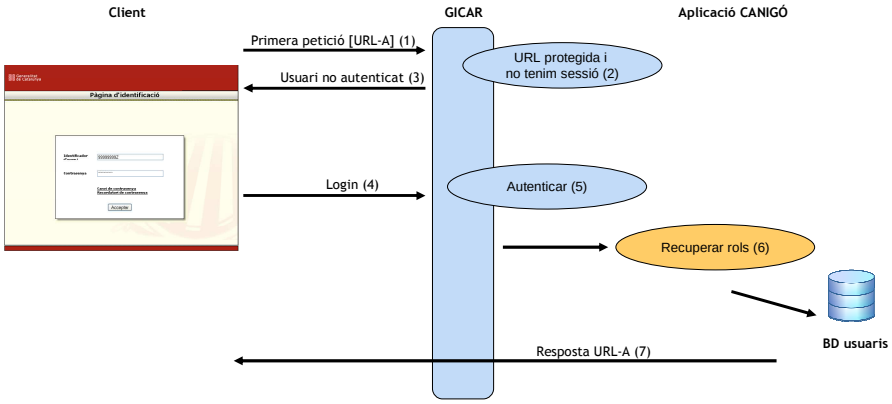
Visió general

El procediment recomanat en aquest how-to per desenvolupar una aplicació que tingui com a requeriment ser desplegada amb autenticació GICAR és:

- Desenvolupar amb Autenticació i Autorització definida a la base de dades
- Activar i configurar el mòdul de GICAR abans de desplegar en un entorn integrat amb GICAR



- Autenticació en desenvolupament (Sense GICAR) -



- Autenticació amb GICAR -

Situació inicial

En aquest document s'ha suposat que ja es disposa d'una aplicació en desenvolupament amb autenticació basada en la definició d'usuaris a la base de dades (tal com s'explica en la documentació del Servei de Seguretat de Canigó)

[1] Gestió d'identitats i control d'accés als recursos

Com desenvolupar una aplicació que requereixi GICAR com a sistema d'autenticació

Passos a seguir per poder desplegar l'aplicació en un entorn securtizat per GICAR

1. Definir el camp de la capçalera de GICAR amb el qual s'obtindrà la clau del nom d'usuari:

Fitxer de configuració	**Canigo-services-security.xml**
Ubicació proposada	<PROJECT_ROOT>/src/main/resources/spring

Definir el bean de GICAR incloent la propietat:

`httpGicarHeaderUsernameKey`

assignant-li el nom del camp del header que es vol fer servir com a identificador de l'usuari. Normalment NIF o CODIINTERN.

```
<bean id="GICARAuthenticationConfiguration"
class="net.gencat.ctti.canigo.services.security.GICARAuthenticationConfigu
ration">
        <property
                name="httpGicarHeaderUsernameKey"
                value="NIF" />
</bean>
```

Exemple de header de GICAR:

HTTP_GICAR=CODIINTERN=NRDRJN0001;NIF=11112222W;EMAIL=mail.admin@gencat.net; UNITAT_MAJOR=CTTI; UNITAT_MENOR=CTTI Qualitat

Com desenvolupar una aplicació que requereixi GICAR com a sistema d'autenticació

2. Activar el sistema de seguretat GICAR (desactivar la resta):

Fitxer de configuració	**Canigo-services-security.xml**
Ubicació proposada	<PROJECT_ROOT>/src/main/resources/spring

Un cop definida la configuració per Gicar, cal afegir-la a la llista de *providers* a la configuració de l'autenticació i modificar les URL's:

- `loginFormUrlValue a "/AppJava/j_acegi_security_check"`
- `authenticationFailureUrlValue a "/gicar-error.html"`

Sense GICAR

```
<beans>
...
<bean id="authenticationConfiguration"
class="net.gencat.ctti.canigo.services.
security.AuthenticationSecurityConfiguration">
 <property name="filterProcessesUrl"
value="/AppJava/j_acegi_security_check"/>

 <property     name="loginFormUrlValue"
               value="/AppJava/pagelogin.do" />

 <property name="authenticationFailureUrlValue"
               value="/AppJava/pagelogin.do" />
 <property name= "authenticationProvidersConfigurationList" >
       <list>
          <!-- <ref local="SACEAuthenticationConfiguration1"/> -->
          <!-- <ref local="LDAPAuthenticationConfiguration2"/> -->
          <ref local= "databaseAuthenticationConfiguration3" />
       </list>
  </property>
</bean>
...
</beans>
```

Amb GICAR

```
<beans>
...
<bean id="authenticationConfiguration"
class="net.gencat.ctti.canigo.services.
security.AuthenticationSecurityConfiguration">
 <property name="filterProcessesUrl"
value="/AppJava/j_acegi_security_check"/>

<property      name= "loginFormUrlValue"
               value="/AppJava/j_acegi_security_check"/>

<property name="authenticationFailureUrlValue"
               value="/gicar-error.html" />
 <property name= "authenticationProvidersConfigurationList" >
       <list>
          <!-- <ref local="SACEAuthenticationConfiguration1"/> -->
          <!-- <ref local="LDAPAuthenticationConfiguration2"/> -->
          <ref local= "GICARAuthenticationConfiguration" />
          <!-- <ref local="databaseAuthenticationConfiguration3"/> -->
       </list>
 </property>
</bean>
...
</beans>
```

Com desenvolupar una aplicació que requereixi GICAR com a sistema d'autenticació

Logoff d'una aplicació

En general, el procediment per fer logoff d'una aplicació amb Canigó consisteix en invalidar la sessió HTTP.

En el cas concret d'autentificació gestionada per Gicar, però, no és suficient amb aquesta acció (que tot i això continua sent necessària) que que d'alguna forma l'aplicació ha de notificar a Gicar la intenció de fer el logoff, de forma que Gicar torni a ddemanar les dades d'identificació de l'usuari en el següent accés.

Per tal de fer logout de GICAR s'ha d'invocar un enllaç de logout. Aquest enllaç de logout és depenent de l'agent de SiteMinder que l'aplicació fa servir per a comunicar-se amb el Policy Server.

Els enllaços de logout són els següents:

- Per a una aplicació ubicada en els apaches corporatius de internet:

  http://sso.gencat.cat/siteminderagent/forms/logoff.html

- Per a una aplicació ubicada en els apaches corporatius de intranet:

  http://sso.gencat.intranet/siteminderagent/forms/logoff.html

- Per a una aplicació amb apache "propi" l'enllaç utilitzat seria el següent:

  http://****.gencat.***/siteminderagent/forms/logoff.html

El procediment general de logoff consistiria llavors en

- Invalidar la sessió en l'aplicació. Això allibera els recursos associats a la sessió i fa que, en el següent accés, s'inicii una nova sessió a partir de les (noves) dades proporcionades per Gicar
- fer un forward a la URL de logoff de Gicar