



TÍCH HỢP HỆ THỐNG SSO

EGOVPLATFORM

TÀI LIỆU KỸ THUẬT

Version 1.1

Copyright© 2014 by OpenEgovPlatform.

LỊCH SỬ PHIÊN BẢN

Phiên bản	Ngày phát hành	Mô tả
1.0	02/09/2014	Mô tả tổng quan về Single Sign On trong hệ thống EgovPlatform
1.1	06/09/2014	Bổ sung hướng dẫn cấu hình cài đặt

GIỚI THIỆU

SSO(Single Sign On) là cơ chế đăng nhập một lần việc này đem lại nhiều thuận tiện cho người dùng và tăng tính năng bảo mật cho hệ thống. Trong hệ thống EgovPlatform có sự dụng cơ chế này và CAS(Central Authenticate Service) chính là một giải pháp SSO trên môi trường Web, đây là một giải pháp mã nguồn mở. CAS sử dụng xác thực liên kết, các hệ thống khác nhau có thể xác thực chỉ một lần thông qua CAS.

Trong nền tảng EgovPlatform có tích hợp với 2 hệ thống quản lý tiến trình công việc (worklow) UEngine và hệ thống báo cáo Pentaho. Đây cũng là 2 hệ thống nguồn mở được tích hợp vào hệ thống nhằm đem lại lợi ích tối đa cho công đồng phát triển e-government.

MỤC LỤC

Thuật ngữ viết tắt	5
1. Tổng quan	6
2. Mô hình tích hợp SSO	7
2.1 Quá trình đăng nhập	7
2.2 Mô hình tiến trình	7
2.3 Single Sign-Out	8
3. Hướng dẫn cấu hình cài đặt	8
3.1 Môi trường cài đặt EgovPlatform	8
3.2 Cấu hình OpenLDAP	9
3.3 Cấu hình CAS	10
3.4 Cấu hình Liferay	11
3.5 Cấu hình UEngine	17
3.6 Cấu hình Pentaho	19
4. Kết luận	21
Tham khảo	22

Thuật ngữ viết tắt

SSO	Single Sign On
LDAP	Lightweight Directory Access Protocol
CAS	Central Authentication Service
JDK	Java Development Kit
J2EE	Java 2 Platform, Enterprise Edition
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
API	Application Programming Interface
CSDL	Cơ Sở Dữ Liệu

1. Tổng quan

Hệ thống EgovPlatform sẽ sử dụng CAS làm hệ thống xác thực login (SSO) chính cho tất cả các ứng dụng được tích hợp mà 2 thành phần tích trong này là UEngine và Pentaho.

CAS cung cấp rất nhiều cơ chế xác thực như:

- CAS URIs,
- CAS Tickets,
- Ticket-Granting Ticket (TGT),
- Service Ticket (ST),
- Proxy Ticket (PT),
- Proxy-Granting Ticket IOU,
- Login Ticket

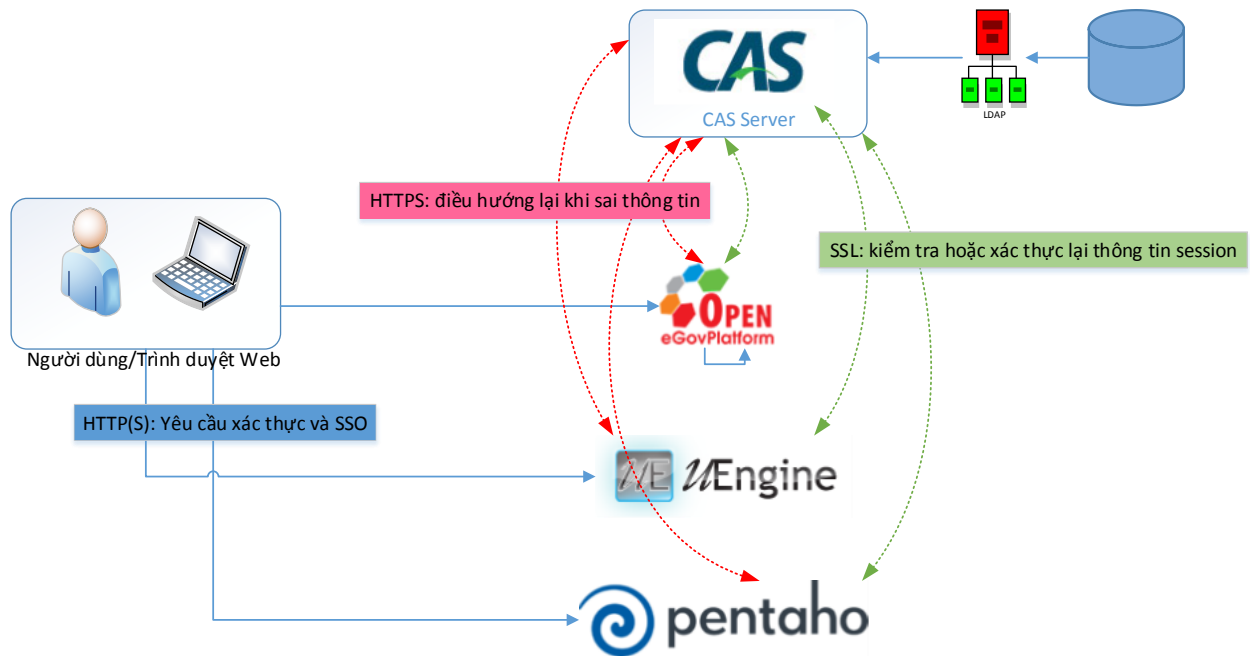
Trong hệ thống EgovPlatform đang sử dụng cơ chế Login Ticket, mục đích sử dụng cơ chế này là ngăn cản sự phản hồi lại thông tin xác thực. Bên cạnh đó việc sử dụng cơ chế này thì cấu hình cũng hết sức đơn giản mà tiện dụng. Bạn có thể tải về tại: <https://www.apereo.org/cas/download>

UEngine là một hệ thống quản lý tiến trình làm việc(workflow), đây là một mã nguồn mở. Giống như các workflow khác, nhưng đây là hệ thống đem lại việc khả chuyển rất mạnh mẽ. Bạn có thể tải về tại: <http://sourceforge.net/projects/uengine/>

Pentaho là một hệ thống báo cáo nguồn mở, hệ thống có khả năng tích hợp với hệ thống CAS mạnh mẽ và tiện dụng. Hệ thống có đủ các tính năng báo cáo như phân tích kinh doanh, tích hợp dữ liệu, dữ liệu lớn. Bạn có thể tải về tại: <http://sourceforge.net/projects/pentaho/>

2. Mô hình tích hợp SSO

Mô hình tổng quan về việc tích hợp SSO vào hệ thống EgovPlatform



Mô hình 1: Mô hình SSO trong hệ thống EgovPlatform

Đây là mô hình mô tả về cơ chế các hệ thống được đăng nhập và xác thực qua CAS. Tất cả hệ thống EgovPlatform, UEngine, Pentaho đều có CAS khách để nhận diện được CAS Server.

2.1 Quá trình đăng nhập

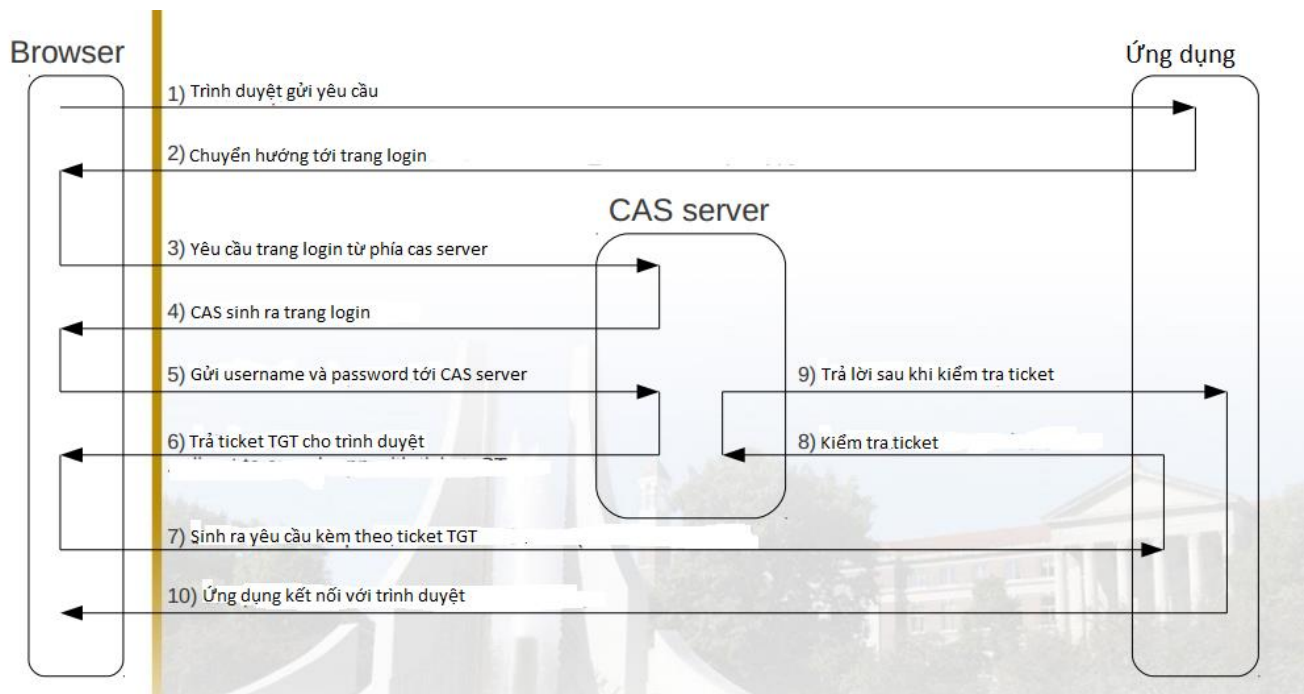
Người dùng duyệt web đăng nhập vào hệ thống EgovPlatform thì sẽ được hệ thống tự động đẩy sang hệ thống CAS Server để xác thực. Khi xác thực thành công hệ thống sẽ sinh ra một vé xác thực vào cửa(ticket). Tất nhiên vé xác thực phải được hệ thống EgovPlatform nhận diện, khi xác thực thành công CAS Server sẽ trả người dùng quay lại hệ thống EgovPlatform để sử dụng dịch vụ, đặc biệt là các dịch vụ công dành cho người dùng này. Tuy nhiên, nếu vé xác thực thông báo là người dùng không đúng, CAS Server cũng sẽ đưa ra thông tin thông báo trên hệ thống để người dùng được biết.

Khi người dùng đã xác thực qua CAS và EgovPlatform người dùng có thể sử dụng hệ thống báo cáo thống kê danh cho mình như Pentaho và nếu người dùng là cán bộ có thể sử dụng hệ thống UEngine

Để làm rõ ràng hơn về việc xác thực ta có thể xem phần tiếp theo

2.2 Mô hình tiến trình

Sau đây sẽ mô tả các bước xác thực qua CAS Server đối với ứng dụng EgovPlatform



2.3 Single Sign-Out

CAS khách có thể truy cập thông tin để kết thúc tiến trình làm việc. Việc này đồng nghĩa tất cả các hệ thống sẽ đồng bộ thoát khỏi tiến trình.

3. Hướng dẫn cấu hình cài đặt

3.1 Môi trường cài đặt EgovPlatform

- Cài đặt trên môi trường Hệ điều hành Linux: Centos 6.4 (64 bit)
- Môi trường JAVA phiên bản: JDK 1.6.0_25. Bạn có thể tải về tại đây: <http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-javase6-419409.html#jdk-6u25-oth-JPR>
- CSDL MySQL phiên bản: Ver 14.14 Distrib 5.1.73.
Để cài đặt bạn có thể dùng lệnh: `yum -y install mysql mysql-server`
- Sử dụng công cụ Apache Directory Studio để quản trị OpenLDAP. Bạn có thể tải về tại đây: <http://directory.apache.org/studio/downloads.html>
- Tải bản cài đặt cas server phiên bản 3.5.0 tại: <http://downloads.jasig.org/cas/> hoặc <https://www.apereo.org/cas/download>
- Tải bản cài đặt liferay jboss phiên bản 6.1.0 GA1 tại: <http://sourceforge.net/projects/lportal/files/Liferay%20Portal/6.1.0%20GA1/>

- Tải bản cài đặt UEngine phiên bản 3.5.4 tại địa chỉ:
<http://sourceforge.net/projects/uengine/files/2.%20uengine%20packaged%20edition/>
- Tải bản cài đặt Pentaho phiên bản 4.5.0 tại địa chỉ:
<http://sourceforge.net/projects/pentaho/files/Business%20Intelligence%20Server/4.5.0-stable/>

3.2 Cấu hình OpenLDAP

- Về thông tin hướng dẫn cài đặt các bạn xem link theo địa chỉ sau:
<http://easylinuxtutorials.blogspot.com/2013/11/installing-configuring-openldap-server.html>
- Ở đây sẽ hướng dẫn bạn cấu hình các thông tin cần thiết để tích hợp với EgovPlatform. Cấu hình như sau:

- o Ở file /etc/openldap/slapd.conf sửa lại thành:
suffix "dc=egovplatform,dc=org"
rootdn "cn=Manager,dc=egovplatform,dc=org"

- o Tạo file init-ldap.ldif với thông tin cơ bản như sau:

dn: dc=egov, dc=org

objectClass: organizationalUnit

objectClass: dcObject

dc: egov

ou: egov.org

dn: cn=Manager,dc=egov,dc=org

objectClass: top

objectClass: organizationalRole

cn: Manager

dn: ou=People,dc=egov,dc=org

objectClass: organizationalUnit

ou: People

#!Tai khoản cho hệ thống EgovPlatform

dn: mail=test@egov.org,ou=People,dc=egov,dc=org

objectClass: top

objectClass: person

objectClass: organizationalPerson

objectClass: inetOrgPerson

cn: Test Test

description::

Y249TmjDs20gTGnDqm0sb3U9R3JvdXBzLGRjPWR0dCvkYz12bg==

givenName: Test

mail: test@egov.org

sn: Test

title: ou=People,dc=egov,dc=org

uid: testegovorg

userPassword:: ZHR0QHRvZGF5

- Sử dụng Apache Directory Studio kết nối với hệ thống OpeLDAP rồi import dữ liệu vừa tạo.
- Bạn sử dụng Apache Directory Studio sửa lại thông tin userPassword.

3.3 Cấu hình CAS

- Bạn có thể xem hướng dẫn cài đặt cấu hình tại đây:
<https://www.liferay.com/web/azar7k1s/blog/-/blogs/sso-via-cas-in-liferay> và
<http://www.liferay.com/community/wiki/-/wiki/Main/CAS+Liferay+6+Integration> , tuy nhiên để tích hợp với EgovPlatform bạn xem như sau:
 - Chỉnh sửa thông tin vào file WEB-INF/cas.properties như sau:
server.name=https://livedemo.openegovplatform.org
server.prefix=\${server.name}/cas
Thông tin log4j như sau:
log4j.config.location=\${jboss.server.base.dir}/deployments/cas.war/WEB-INF/classes/log4j.xml
 - Chỉnh sửa thông tin vào file WEB-INF/deployerConfigContext.xml như sau:
Ở trong thẻ <property name="authenticationHandlers"> bổ sung(nếu có thì chỉnh sửa lại) thông tin như sau:

```
<bean class="org.jasig.cas.adapters.ldap.BindLdapAuthenticationHandler" >  
  <property name="filter" value="mail=%u" />  
  <property name="searchBase" value="ou=People,dc=egov,dc=org" />  
  <property name="contextSource" ref="contextSource" />  
  <property name="ignorePartialResultException" value="yes" />  
</bean>
```

Và:

```
<bean id="contextSource"
class="org.springframework.ldap.core.support.LdapContextSource">
    <property name="pooled" value="true"/>
    <property name="urls">
        <list><value>ldap://ldap.egov.org:389</value></list>
    </property>
    <property name="userDn" value="ou=Manager,dc=egov,dc=org"/>
    <property name="password" value="$demoegov$"/>
    <property name="baseEnvironmentProperties">
        <map>
            <entry>
                <key>
                    <value>java.naming.security.authentication</value>
                </key>
                <value>simple</value>
            </entry>
        </map>
    </property>
</bean>
```

Thông tin ở đây tương ứng với thông tin bạn đã cài đặt trên OpenLDAP

- Bây giờ bạn có thể khởi động hệ thống và kiểm tra, nếu đăng nhập sai sẽ có thông báo hiển thị trên màn hình

3.4 Cấu hình Liferay

- Hướng dẫn cài đặt có thể xem tại đây: <https://www.liferay.com/documentation/liferay-portal/6.1/user-guide/-/ai/lp-6-1-ugen11-installing-liferay-on-jboss-7-0> hoặc <https://www.youtube.com/watch?v=43RgsxwBVBk>
- Hướng dẫn cấu hình Liferay với OpenLDAP và CAS như sau:
 - Cấu hình CAS:
Nhập thông tin cấu hình theo hình, chỉnh sửa thông tin cho phù hợp với CAS

Xác thực

Trạng thái chung

LDAP

CAS

Facebook

NTLM

OpenID

Mở SSO

Người quản lý Site

☒ Cho phép
 ☒ Nhập dữ liệu từ LDAP

URL đăng nhập

URL đăng xuất


Tên máy chủ

URL máy chủ

Service URL

Không có URL chuyển tiếp với người sử dụng này

Kiểm tra cấu hình CAS


LIFERAY
Enterprise Open Source For Life

Open EgovPlatform

Cấu hình
[Trạng thái chung](#)

Xác thực
[Người dùng](#)
[Tên máy chủ thư](#)
[Thư điện tử thông báo](#)

Nhận dạng
[Địa chỉ](#)
[Số điện thoại](#)
[Các địa chỉ thư điện tử khác](#)
[Trang web](#)

Cấu hình khác
[Hiện thị cài đặt](#)
[Các ứng dụng của google](#)

Ghi lại

Hủy bỏ

Kiểm tra thông tin:

CAS

URL đăng nhập:

☒ Đã qua
 ☐ Chưa qua
 ☐ Chưa kiểm tra

URL đăng xuất:

☒ Đã qua
 ☐ Chưa qua
 ☐ Chưa kiểm tra

URL máy chủ:

☒ Đã qua
 ☐ Chưa qua
 ☐ Chưa kiểm tra

https://livedemo.openegovplatform.org/cas/login

https://livedemo.openegovplatform.org/cas/logout?service=http://livedemo.openegovplatform.org/group/guest/trang-chu

https://livedemo.openegovplatform.org/cas

- Cấu hình LDAP:
Chọn thông tin cấu hình cơ bản

Xác thực

Trạng thái chung

LDAP

CAS

Facebook

NTLM

OpenID

Mở SSO

Người quản lý Site



☒ Cho phép

☐ Bắt buộc

Máy chủ LDAP

Thêm

EGOV_LDAP



Nhập/Xuất

☐ Nhập dữ liệu được kích hoạt

☒ Kích hoạt Xuất ra

Quy định về mật khẩu

☐ Sử dụng quy định mật khẩu của LDAP

LIFERAY
Integrating Open Source For Life

Open EgovPlatform

Cấu hình

[Trạng thái chung](#)

Xác thực

[Người dùng](#)

[Tên máy chủ thư](#)

[Thư điện tử thông báo](#)

Nhận dạng

[Địa chỉ](#)

[Số điện thoại](#)

[Các địa chỉ thư điện tử khác](#)

[Trang web](#)

Cấu hình khác

[Hiện thị cài đặt](#)

[Các ứng dụng của google](#)

Ghi lại

Hủy bỏ

Nhập thông tin OpenLDAP Server gồm:

Tên máy chủ và thông tin Kết nối

Tên máy chủ


EGOV_LDAP

Các giá trị mặc định

- ☐ Apache Directory Server
- ☐ Fedora Directory Server
- ☐ Microsoft Active Directory Server
- ☐ Novell eDirectory
- ☐ OpenLDAP
- ☐ Máy chủ thư mục khác

Khởi tạo lại giá trị

Kết nối

Liên kết của nhà cung cấp 

ldap://dap.egov.org:389

Base DN 

ou=People,dc=egov,dc=org

Quy tắc

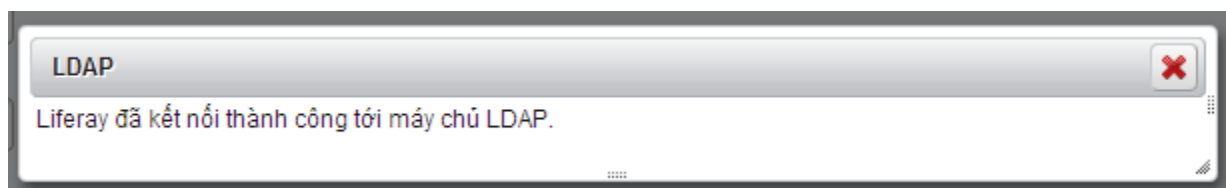
ou=Manager,dc=egov,dc=org

Chứng nhận

.....


Kiểm tra kết nối LDAP

Kiểm tra kết nối



Thông tin người dùng

Người dùng

Bộ lọc xác thực tìm kiếm 

(mail=@email_address@)

Nhập dữ liệu bộ lọc tìm kiếm

(objectClass=person)

Ảnh xạ người dùng

Tên hiển thị

uid

Mật khẩu

userPassword

Địa chỉ thư điện tử

mail

Tên đầy đủ 

cn

Tên

givenName

Tên đệm

Họ

sn

Tên công việc

Chân dung

Nhóm

description

UUID

Kiểm tra người dùng LDAP

Thông tin nhóm người dùng

Các nhóm

Nhập dữ liệu bộ lọc tìm kiếm

Group Mapping

Tên nhóm

Mô tả

Người dùng

Thông tin xuất sang LDAP

Xuất

Users DN

Lớp người dùng mặc định

Groups DN

Group Default Object Classes

Lưu lại các thông tin sau khi sửa đổi

- Sau khi tất cả các thông tin lưu thành công thoát ứng dụng đăng nhập lại, hệ thống sẽ lập tức chuyển quá trình đăng nhập sang hệ thống CAS. Sau đó dùng account đã tạo trong OpenLDAP để đăng nhập lại.

3.5 Cấu hình UEngine

- Chỉnh sửa file tài về thành uengine-web.war, copy vào thư mục deployments của liferay
- Cấu hình các thông số như sau:

- o Thông số kết nối CSDL

uengine-web.war/WEB-INF/classes/org/uengine/**uengine.properties**

Thay đổi thông số phù hợp với CSDL của bạn

datasource.jndiname=java:/uEngineDS

jdbc.driverClassName=com.mysql.jdbc.Driver

jdbc.url=jdbc:mysql://localhost:3306/{**uengine**?autoReconnect=true&characterEncoding=UTF-8

web.url=http://localhost:8080/uengine-web

jdbc.username={**username**}

jdbc.password={**password**}

- o Thông số kết nối CAS trong file uengine-web.war/WEB-INF/**web.xml**

Thay đổi thông tin phù hợp với hệ thống CAS của bạn

<filter>

<filter-name>CAS Single Sign Out Filter</filter-name>

<filter-class>org.jasig.cas.client.session.SingleSignOutFilter</filter-class>

</filter>

<filter>

<filter-name>CAS Authentication Filter</filter-name>

<filter-class>org.jasig.cas.client.authentication.AuthenticationFilter</filter-class>

<init-param>

<param-name>casServerLoginUrl</param-name>

<param-value>**https://livedemo.openegovplatform.org/cas/login**</param-

value>

</init-param>

<init-param>

<param-name>serverName</param-name>

<param-value>**http://livedemo.openegovplatform.org**</param-value>

```
</init-param>
</filter>
<filter>
  <filter-name>CAS Validation Filter</filter-name>
  <filter-class>org.jasig.cas.client.validation.Cas10TicketValidationFilter</filter-
class>
  <init-param>
    <param-name>casServerUrlPrefix</param-name>
    <param-value>https://livedemo.openegovplatform.org/cas</param-value>
  </init-param>
  <init-param>
    <param-name>serverName</param-name>
    <param-value>http://livedemo.openegovplatform.org</param-value>
  </init-param>
</filter>
<filter>
  <filter-name>CAS HttpServletRequest Wrapper Filter</filter-name>
  <filter-class>org.jasig.cas.client.util.HttpServletRequestWrapperFilter</filter-
class>
</filter>
<filter>
  <filter-name>CAS Assertion Thread Local Filter</filter-name>
  <filter-class>org.jasig.cas.client.util.AssertionThreadLocalFilter</filter-class>
</filter>
<!-- Sign out not yet implemented -->
<filter-mapping>
  <filter-name>EncodingFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
<filter-mapping>
  <filter-name>CAS Single Sign Out Filter</filter-name>
  <url-pattern>/*</url-pattern>
```

```
</filter-mapping>
<filter-mapping>
    <filter-name>CAS Authentication Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<filter-mapping>
    <filter-name>CAS Validation Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<filter-mapping>
    <filter-name>CAS HttpServletRequest Wrapper Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
<filter-mapping>
    <filter-name>CAS Assertion Thread Local Filter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

3.6 Cấu hình Pentaho

- Hướng dẫn cài đặt bạn có thể xem chi tiết tại đây:
<http://anonymousbi.wordpress.com/2012/10/28/pentaho-bi-server-4-5-0-definitive-mysql-installation-guide/>
- Sau đây sẽ hướng dẫn cấu hình Pentaho vào CAS như sau:

- o Tìm file Pentaho/pentaho-solutions/system/**applicationContext-spring-security-cas.xml**

Thông số **serviceProperties**

```
<bean id="serviceProperties"
class="org.springframework.security.ui.cas.ServiceProperties" autowire="default"
dependency-check="default" lazy-init="default">

    <property name="service"
value="http://livedemo.openegovplatform.org/pentaho/j_spring_cas_security_check"/>

    <property name="sendRenew" value="false"/>

</bean>
```

Thông số **casProcessingFilterEntryPoint**

```
<bean id="casProcessingFilterEntryPoint"
class="org.springframework.security.ui.cas.CasProcessingFilterEntryPoint"
autowire="default" dependency-check="default" lazy-init="default">
    <property name="loginUrl"
value="https://livedemo.openegovplatform.org/cas/login"/>
    <property name="serviceProperties">
        <ref local="serviceProperties"/>
    </property>
</bean>
```

Thông số **ticketValidator**

```
<bean id="ticketValidator"
class="org.jasig.cas.client.validation.Cas20ServiceTicketValidator"
autowire="default" dependency-check="default" lazy-init="default">
    <constructor-arg index="0"
value="https://livedemo.openegovplatform.org/cas" />
</bean>
```

Thông số **logoutFilter**

```
<bean id="logoutFilter"
class="org.springframework.security.ui.logout.LogoutFilter" autowire="default"
dependency-check="default" lazy-init="default">
    <constructor-arg
value="https://livedemo.openegovplatform.org/cas/logout?service=http://livedemo
.openegovplatform.org/pentaho"/>
    <constructor-arg>
        <list>
            <bean
class="org.pentaho.platform.web.http.security.PentahoLogoutHandler"/>
            <bean
class="org.springframework.security.ui.logout.SecurityContextLogoutHandler"/>
        </list>
    </constructor-arg>
    <property name="filterProcessesUrl" value="/Logout"/>
</bean>
```

- Sau đó khởi động lại Server Pentaho và Liferay

- Tạo tài khoản trong Pentaho tương ứng với tài khoản trong liferay và phân quyền cho tài khoản có quyền xem hay quản trị báo cáo.

4. Kết luận

Trong nền tảng mở openegovplatform ta có thể tích hợp được với rất nhiều hệ thống khác mà có hỗ trợ SSO, trên ta dùng UEngine và Pentaho chỉ là 2 hệ thống mở rộng. Tài liệu này cũng mô tả một cách khái quát mà không đi sâu xa vào từng chi tiết kĩ thuật của từng hệ thống, chỉ nhằm mô tả được cơ chế tích hợp SSO mà EgovPlatform có thể sử dụng. Việc EgovPlatform SSO sẽ đem lại tiện ích tối đa đối với các hệ thống đang dùng sẵn có mà không phải thay đổi nhiều về mặt phát triển.

Các thành phần trên nhằm khẳng định rằng EgovPlatform không những mở cả về mặt kĩ thuật lẫn công nghệ mà còn mở cả mặt tư tưởng cho các nhà phát triển.

Tham khảo

- <http://openegovplatform.org>
- <https://vietvo.wordpress.com/2010/09/12/single-sign-on-solution/#more-999>
- <http://uengine.org>
- <http://www.pentaho.com>
- <https://www.apereo.org>
- <http://www.openldap.org>