IAIC Transactions on Sustainable Digital Innovation (ITSDI)
Vol. 1 No. 2 April 2020

p-ISSN: 2686-6285
e-ISSN: 2715-0461

Comparison of CAS and Manage Oauth in Single Sign on (SSO) Client Applications

Sri Watini[1], Pipit Nursaputri[2], Muhammad Iqbal[3]
STKIP Panca Sakti Bekasi[1] , Universitas Raharja[2,3]
Indonesia
e-mail: srie.watini@gmail.com[1] , pipit.nursaputri@raharja.info[2] , iqbal@raharja.info[3]

Author Notification
28 April 2020
Final Revised
28 April 2020
Published
29 April 2020

(APA style, Justify, Arial 10pt) Example:
To cite this document:
Watini, S., Nursaputri, P., & Iqbal, M. (2020). Comparison of CAS and Manage Oauth in Single Sign on (SSO) Client Applications. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 152-159. https://doi.org/https://doi.org/10.34306/itsdi.v1i2.147

Abstract

Single Sign On is one of the systems that have been developed long ago to meet the expectations of developers to provide ease and convenience of accessing data. In the development of the system, methods and protocols have been formed in varied ways to suit the needs of the developers . In a variety of methods and protocols , a developer can choose the architecture and protocols that can be used to develop the system. Central Authentication Service and Open authorization is two Single Sign On systems most widely used in the manufacture of a web log . Both can be used as the basis for the application of the system of Single Sign On for developers who intend to design a login system that is safe and comfortable , so that developers can create a system that suits his desire .

Keywords: Central Authentication Service, Open Authorization, Single Sign On, Php

1. Introduction

Web is a media interface that is made in such a way as to provide comfort and the ease of accessing information available on the internet. The development of a web can not be separated from the development of existing systems therein, one of which is the login system which is now starting to become a concern for the parties web developer. Where the comfort and safety of the web are created along with web development itself. Granting access rights is the basis of the login system, where each user can or not to access an information that depends on the rights received. (Al-Fedaghi 2011).

Single Sign On is a system created to make it easy for users, where users only need to log in just once in order to access the whole application that has been integrated with the SSO protocol. So that developers compete in maximizing the login system on the web they develop, where there are many methods that can be used and protocols that can be implemented. (Grag 2016.)

Aminudin (2014) in his thesis entitled "Implementation of Single Sign On (SSO) Support For E-Commerce Interactivity Applications Using Oauth Protocol " states that by using SSO, users only simply try to authentication only once to get permission, access to all services contained in network. Using the OAuth protocol, users can authorize clients to access protected data already on the server by giving a token without file username and password. OAuth allows users to provide access to third party sites to access information stored on service providers without having to share access rights or all their data. Single Sign On system with OAuth protocol used is authentication technology with a token code not a username and password. This research is expected to make it easier for users to authenticate e-commerce applications using an account provider that supports the protocol OAuth, so it's a positive effect on trading.

2. Research Method

From this study it will be known the ease of designing a web login between CAS and OAuth as a basis for SSO which refers to journals, articles, theses and easy tutorials in making the login system, as well as how the process of the central authentication login system service and open authorization as a login system in SSO. Making this web login based on the needs of the two systems that will serve as examples, where default configuration for cas and simple web login with google account for oauth. Test the performance of the login system between CAS and OAuth using Apache Bench, test What is done is Response Time, where in this test the second performance will be a known login system to handle requests per unit second. Apache Bench tools can be opened via cmd, after entering the path C: \ xampp \ apache \ bin, the command is entered as> ab –t [time (s)] [http: //] hostname [: port] / path. Here the results can be observed is the number of requests that can be handled by the system in the time interval that has been determined.

2.1 TOOLS AND MATERIALS

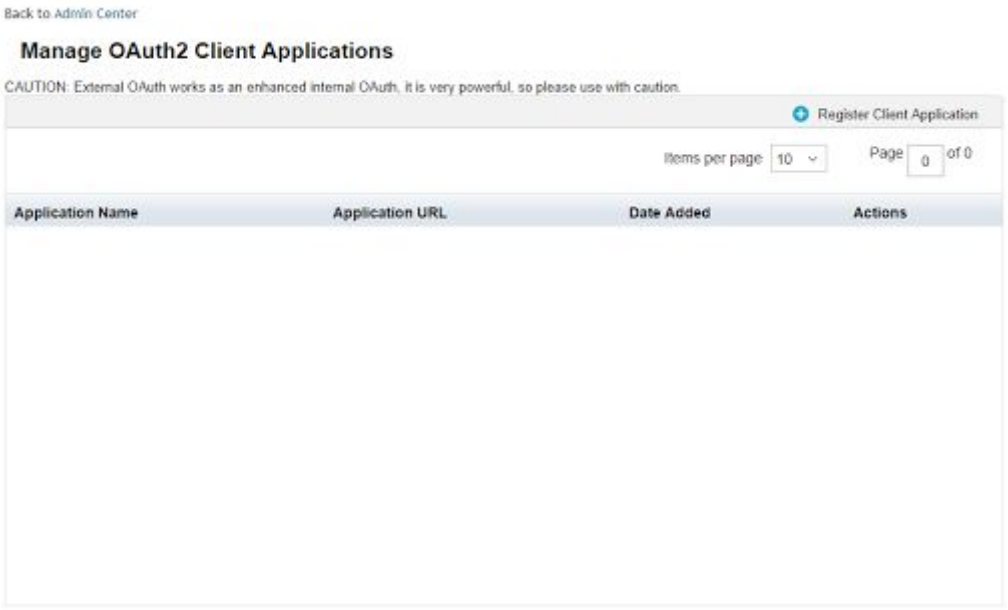
The main equipment in this study is divided into two categories, namely hardware (hardware) and software (software). The hardware used is the Acer Laptop ASPIRE E1-471 with Windows 7 operating system and Intel Core i3 Processor specifications 2328M up to 2.2GHz, 500GB hard disk and 2GB RAM. Software used for research is Apache, PHP, Mysql, Tomcat 7.0.56, Mozilla Firefox.

3. Findings

3.1 Research Implementation

After creating the Central Authentication Service and Open Authorization web login is complete, then an attempt to log in with a username and password by default for Central Authentication Service and login with a google account for Open Authorization.

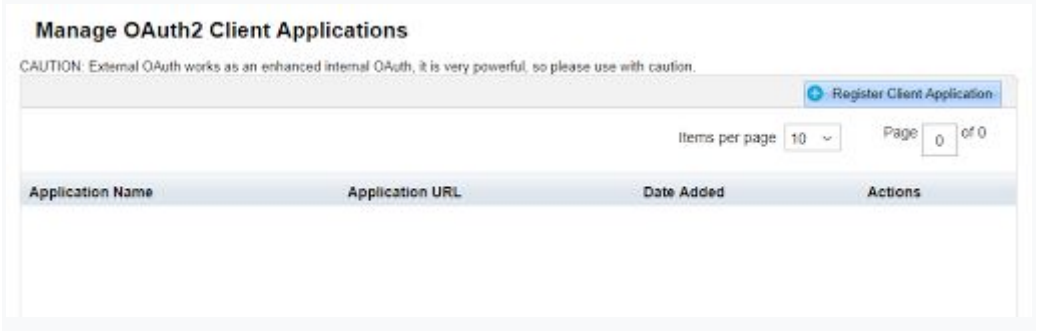
1. So, in view of the title, Manage OAuth2 Client Applications, this section is used to manage the authorization process for any application made by the company or existing, so that employees can register using the SAP Success Factor site account. As with other sites that can authorize with a Facebook or Google account.



Picture 1. initial display

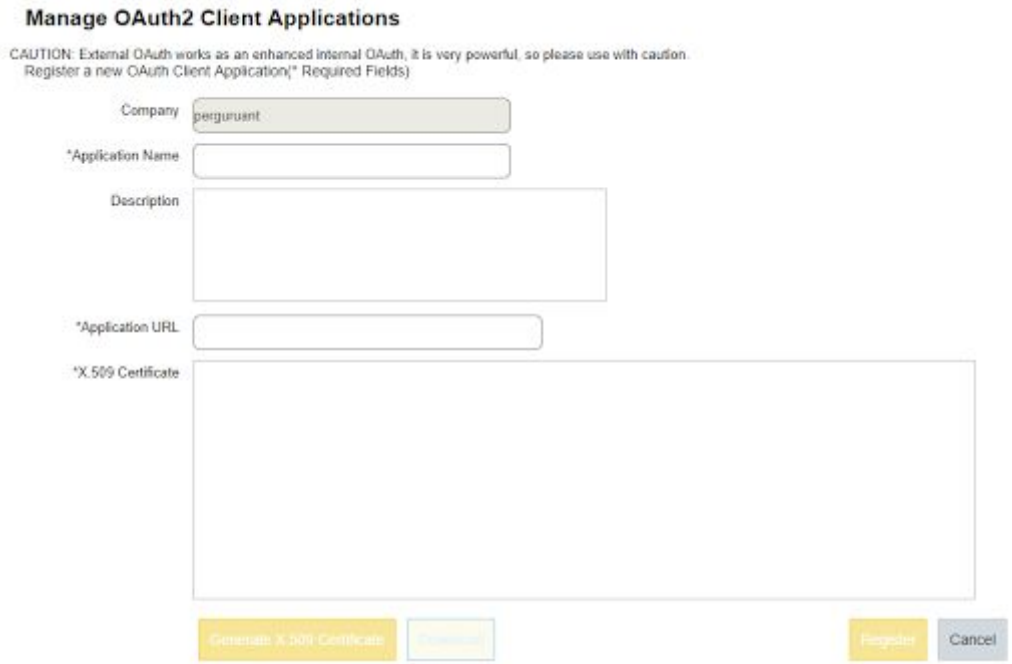
2. In this manager section we can set any application that will link to this site, including the address of the application. If we want to register the application, we

just need to click Register Client Application then fill in the form listed there.



Picture 2. register menu client

3. The parts that must be filled in the form include the name of the application that we are going to register, then describe the application as what and for what, then the URL address of the application and a certificate that the application has been released and then click Register.



Picture 3. register menu

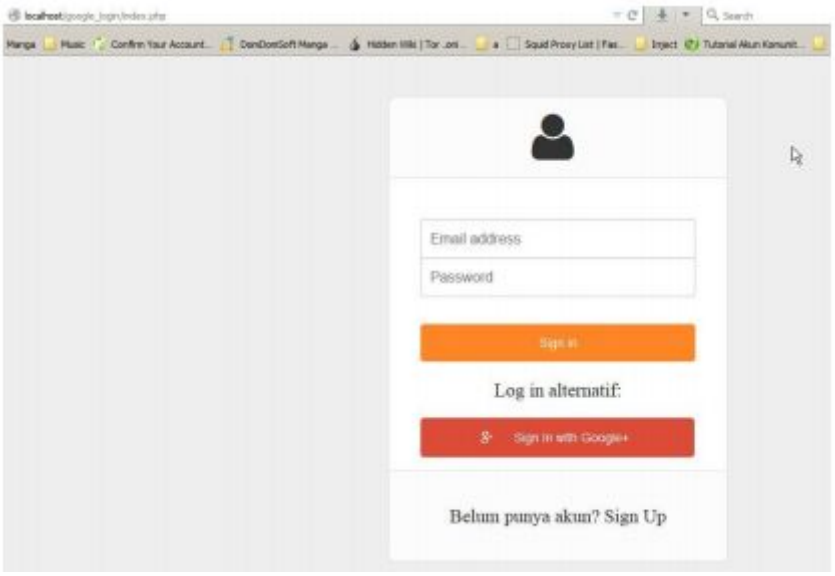
Then in the Manage OAuth2 Client Application view, there is a table with fields for the

p-ISSN: 2686-6285
e-ISSN: 2715-0461

name of the application, the URL address of the application that is registered and when the application was added, and actions that can be taken against the application whether to disable access rights to the application or not.

3.2 Login to the Oauth web login

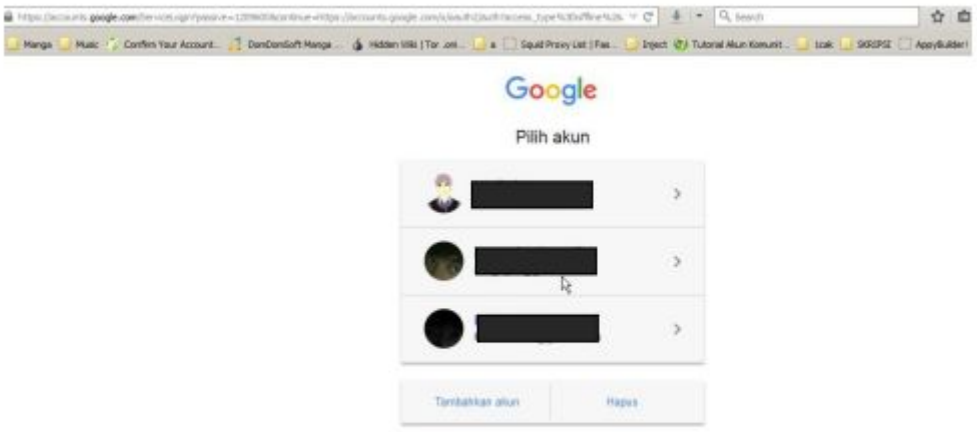
Access the localhost / google_login address, so a simple login form screen will appear where there are two fields for email address and password. One Sign in and one button Sign in with Google+ button. The Sign in button is an ordinary login button, whereas Sign in with Google+ button is integrated with the Oauth system so that users will be directly forwarded to the user's google account.



Picture 3. Display Login Page of OAuth

The google account that will appear after the Sign in with Google+ button is clicked, appears user-owned accounts. Select a user and click to enter password.

p-ISSN: 2686-6285
e-ISSN: 2715-0461



Picture 4. Display of Available Google Accounts

A page will appear asking for the user's Google account password, if the user is logged in with his Google account he will automatically be given access from the web he wants to access.

Picture 5. Google Account Login

Home page / home after logging in, if the user does not log out of his google account then automatically when the user accesses the localhost / google_login address it will automatically directly direct to halman home.

Picture 6. Display Page After Login

4. Conclusion

From the research that has been done, several conclusions can be drawn including:
1. CAS is more difficult to implement as SSO in web login than OAuth, because of the complexity of the CAS system and the lack of popularity of this system as well as the lack of tutorial support.
2. OAuth is easier to implement in SSO, aside from its easy configuration and the development of OAuth, also because in its development OAuth is far more numerous used by most developers. The number of tutorials and developer interests for developing this OAuth login system makes it even easier to make the system OAuth login.
3. In the ability to receive requests, CAS is far better than OAuth, where the greater the delay time, the greater the number of requests that can be handled.

References

[1] Aminudin. (2014). Implementation of Single Sign On (SSO) Support For E-Commerce Interactivity Applications Using Protocol Oauth. GAMMA, Vol 10, No 1 (2014).

[2] Amarudin. (2014). Implementation of CAS Server as Authentication Protocol on Single SignOn(SSO) Network With PHP Programming. ICETIA. Informatics Engineering Department STMIK Teknokrat.

[3] Grag, Parul. (2016). SSO (Single Sign On) Implementation. International Journal of Science and Research (IJSR), Volume 5 Issue 6, June 2016.

[4] Muni. (2016). Login with Google OAuth 2 Using PHP and MySQL. Retrieved July 15, 2016, from http://www.smarttutorials.net/login-with-google-oauth-2-using-php-and-mysql.

[5] Ramadhan, Gilang. (2013). Analisis teknologi Single Sign On (SSO) dengan penerapan Central Authentication Service (CAS) pada Universitas Bina Darma. Bina Darma e-Journal, Vol. xx No.x Oktober 2013: 1-13.

[6] Kurniawan, Fite., Fajar Suryawan., & Umi Fadlilah. (2014). Membangun Privileges Pada Jaringan Komputer Sma Negeri 2 Boyolali Berbasis Active Directory Dengan Windows Server 2008 Enterprise. Emitor, Volume 14 No. 1, Maret 2014.

[7] Al-Fedaghi, Sabah. Developing Web Applications. International Journal of Software Engineering and Its Applications, Vol.5 No.2, April, 2011

[8] Aini, Q., Rahardja, U., & Naufal, R. S. (2018). Penerapan Single Sign On dengan Google pada Website berbasis YII Framework. *Sisfotenika*, *8*(1), 57-68.

[9] Rahardja, U., Aini, Q., & Sulastrini, L. R. (2017). Penerapan Inbound Official Site Sistem Informasi Untuk Meningkatkan Rank Webometrics. *Technomedia Journal*, *1*(2), 105-115.

[10] Yusup, M., Aini, Q., Apriani, D., & Nursaputri, P. (2019, December). PEMANFAATAN TEKNOLOGI BLOCKCHAIN PADA PROGRAM SERTIFIKASI DOSEN. In *SENSITIf: Seminar Nasional Sistem Informasi dan Teknologi Informasi* (pp. 365-371).