Implementation of Indirect Single Sign-On Approach to Integrate Web-Based Applications

Rinta Kridalukmana[1], Kodrat Iman Satoto[2]

**[1,2] Department of Computer Engineering, Diponegoro University
Semarang, 50275, Indonesia**

Abstract

Managing user credential is a critical point in organization that has application island environment such as Diponegoro University. By so doing, application users will be helped to keep only one login information for entering those applications. Not changing login function in each application is the boundary that has been set when managing credentials. For this reason, indirectly single-sign-on approach is used in this research. Meanwhile, applications will be integrated using presentation integration model in web based environment. Using CodeIgniter Framework, single-sign-on portal has been developed to handle single login to applications available in Diponegoro University. As the result of this research, we found that by using indirectly single-sign-on approach almost all session variables from secondary domain application can work well under primary domain application except the secondary application that uses a dynamic variable session key. This circumstance will impact a logging out process when user signs out from primary domain application.

Keywords: *Indirectly Single Sign On, Manage User Credential, Presentation Integration.*

1. Introduction

The need of Diponegoro University for the application of information system to support the processes of monitoring, evaluation, and effective and efficient operation is increasing. In response to this need, any web-based applications have been developed in consideration to the facilitation of accessible location and acceleration of distributing process for any parties requiring. Those applications that have been developed include Academic Information System, Personnel Information System, Executive Information System, Budget Information System and other applications that are developed to support the evaluation of a teaching-learning process.

However, a part from the development of those applications both in the side of quantities and the one in service facilitating the users to access information in Diponegoro University environment, it in fact still emerges certain drawbacks for the application users as they have to memorize a lot of information of user login for each of application. This drawback is so significantly prominent – particularly for those unfamiliar with the interaction of information technology and those mostly relatively old in age. Moreover, each of web-based application has its own different URL address that sometimes does not use the domain name to ease the access but using *IP address*.

In fact, such condition occurs not only in Diponegoro University environment but also in any other organizations. Of the cases occurred in the external environment, the most widely used solution is by using single-sign-on approach in which a user not merely has *credential* but she or he can access a number of applications in accordance with his or her rights. This solution can be used as a model to be applied in the environment of Diponegoro University. Hence, the indirect single sign-on approach is used in this research purposely to access any services of web-based information system application. The application of indirect single sign-on is conducted by developing the portal of single-sign-on (SSO Portal) which becomes the primary domain that can be used to link to any other existing applications that, in turn, is called as secondary domain application. The SSO Portal in addition acts as a *presentation integrator* for any services of secondary domain application. The indirect single sign-on approach is chosen in consideration to the existing limitation that the secondary domain application has no any changes of logical functions. As a result of this limitation, the application service having a login function using *Captcha* has still not been integrated to the SSO Portal.

2. Literatures

2.1 Management of Single User Sign-On

Single sign-on is defined as a mechanism in which a user only with authenticating action can be allowed to access all computers and the system is in line with his or her access rights without any need to use the passwords repeatedly [7][1][3].

Fig 1 illustrates that the distributed system historically has some components functioned as the independent security domains. These components have their own platform, each of which is connected to the operational and applicative system and acts as an independent domain in the sense that an end-user must be identified and independently authenticated to each accessed domain.

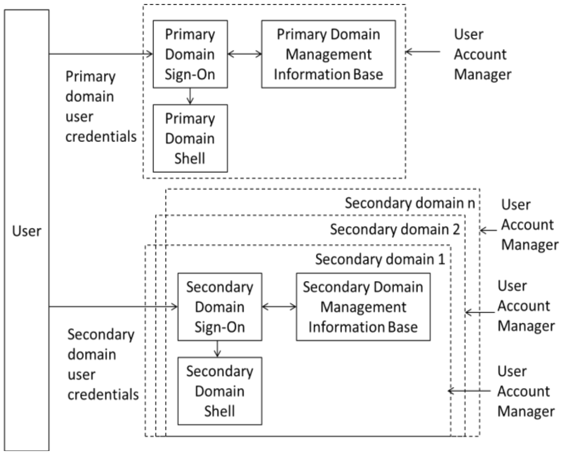


Fig. 1 - User Sign-On to Multiple Systems [7]

Initially, the user will interact with the primary domain to make a session in primary domain. To do so, the user must give a credential that is suitable with primary domain. Furthermore, to have the service in secondary domain, a user is required to again login by using credential suitable for the primary domain.

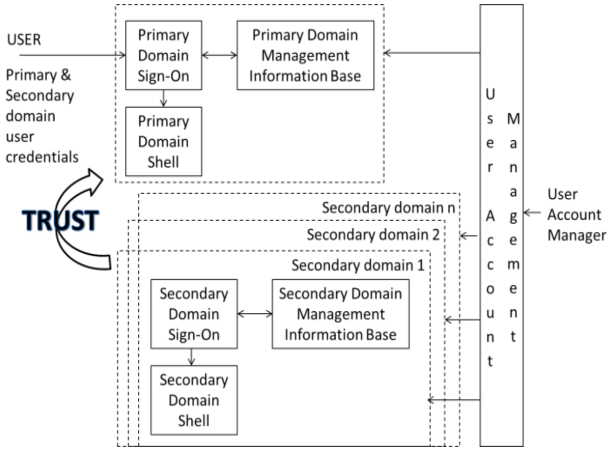


Fig. 2 - Single User Sign On to Multiple Services [7]

By using the model of single user sign-on as shown in Fig. 2, the information given by the users a part of the procedures of sign-on in primary domain can be used in secondary domain through a number of the following ways:

1) *Directly* – information given by the user is directly sent to the secondary domain as a part of secondary domain.
2) Indirectly - information given by the user is used to retrieve the user identification and the credential user information stored in single sign-on management information base. The result of retrieval information further is used as a base for sign-on operation in secondary domain
3) Immediately – It is by making session in the secondary domain when initial session is performed when signing–on to primary domain.
4) Information of user sign-on is temporarily stored or stored in cache and is used when there is a request to the secondary domain by users.

The security aspect that needs to be underlined in single sign-on model is that the secondary domain must believe in the primary domain to identify the user credentials [5] and must do authentication and protect the information of the credential users from any abuse.

2.2 Code Igniter Framework

CodeIgniter refers to a framework to help any development of web-based application using programming language of PHP [2]. The aim of this framework development is to develop the acceleration of application development by providing a group of libraries frequently needed in doing certain function. Using the approach of Model-View-Controller (MVC), it is possible to separate between logical function and the display of the application. In its application, this approach makes possible for a web page to contain a script of web page as minimal as possible as it is separated from the PHP script.

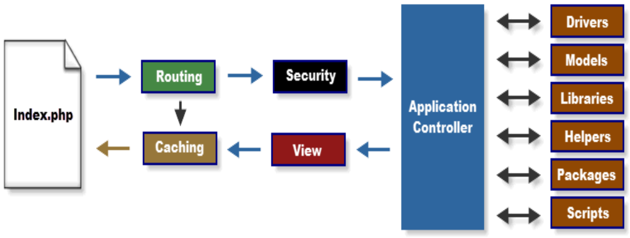


Fig. 3 – Code Igniter Framework Application Flowchart [2]

Fig 3 shows that in CodeIgniter framework, the file of index.php serves as a front controller that will initiate the resource required to operate. Subsequently, Router will check HTTP request in order to determine what will be done from the request. If the cache file exists, it will be directly sent to the browser by normally executing the system. Prior to the calling of application controller, HTTP request and the data sent by the user will be firstly filtered for security.

Furthermore, the controller will call model, core libraries, helpers, and other resources required to processing certain requests. As a result, the view will be rendered and sent to the browser web to be presented. If the caching is activated, the view will be firstly saved in the cache; thus when there is an order request, it can be serviced well then.

2.3 Integrated Application Model

Database technology can solve some parts of problem using a traditional approach. One more accurate definition for the database refers to a group of data managed to service some applications efficiently using data centralization and minimizing the data redundancies [4]. William Tse mentions that there are, at least, 3 (three) models in the application integration [8][6], including:

1) Integration of presentation. It is a user interface providing an access in an application. Such model of presentation integration can be seen in Fig 4. The benefits of the model of presentation integration are related to the low risk and cost, relatively stable availability of technology, simplicity in use, and fast implementation without any needs to change the data source. By contrast, it has some weaknesses particularly in performance, perception and unavailability of interconnection between application and data.

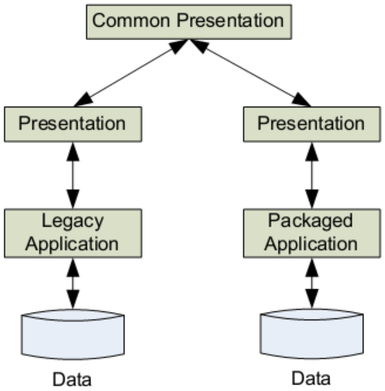


Fig. 4 - Model of Presentation Integration, William Tse [8]

2) Data Integration refers to a model of data integration that is directly done in database or data structure from the application by ignoring the presentation and business logic when making integration. Fig.5 illustrates the model of data integration.

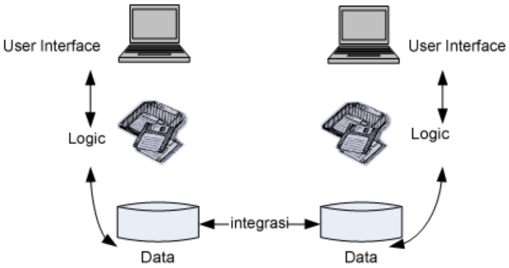


Fig. 5 - Model of Data Integration, William Tse [8]

The strength of this model is related to its better flexibility from the presentation model and it can make the data possible to be used by other applications. However, if there is a change in data model, the integration, as a consequence, will no longer be active.

3) Functional Integration – It is done at the level of business logic by using the distributed processing middleware. Fig 6 illustrates the model of functional integration. The strength of this model is related to its strong integration capability among other integration models. Besides, this model uses true code reuse infrastructure to several applications in enterprise. Yet, there are some drawbacks of this model in its implementation such as from the cost or time in view of high complexity.

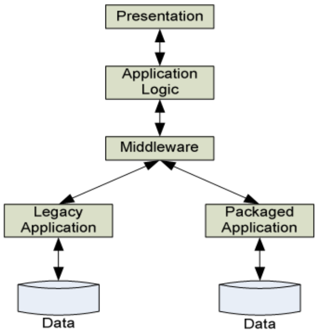


Fig.6 - Model of Functional Integration William Tse [8]

3. Use Case Model and Process Design

3.1 Brief Description of Portal Single Sign On

Indirect Single Sign-On is one of approaches to manage the credential user to each of application in secondary domain application by storing it as the user information base. Further, when a user will access the secondary domain application, he or she will do a searching in the user information base to check whether the user has a right to enter the secondary domain application.

In its implementation, SSO portal will act to save the user information base. As the user uncertainly has an access to all applications in secondary domain application, SSO portal also provides a page of control panel to ease the user to select the application in accordance with the right he or she has. To illustrate this, a lecturer has a right to access to academic application but not all of lecturers have an access to finance application. Thus, the lecturer through the control panel page can register the credential user only for the academic application or simultaneously to register to credential user for the finance application if he or she has an access for the user information base.

In addition to that, SSO portal also provides a menu of navigation to select which secondary domain application will be accessed. When one of the navigation menus is chosen, he or she will do a request login to secondary domain application based on the user information base that has been saved. The user is able to select which the secondary domain application will be displayed in navigation menu considering that a user perhaps does not have any access to all secondary domain applications. .

SSO portal is developed to manage single-sign-on to 18 web-based applications available in the environment of Diponegoro University, including:

1) Webmail Application
2) System for Personnel Information
3) System for Executive Information
4) System for Academic Information
5) Billing System
6) Evaluation System for Teaching-Learning Process
7) Evaluation System for Lecturing Data
8) System for Higher Education Accreditation
9) System for Quality Target
10) System for Online Lecture
11) System for Online Registration
12) System for Entrance Examination
13) Budget System
14) System for Career Development Center (CDC)
15) System for Host-to-host Mandiri Bank
16) System for Host-to-host BNI Bank
17) System for Host-to-host BRI Bank
18) System for Host-to-host BTN Bank

3.2 Use Case Diagram

As explained in problem background, SSO portal in a broad line has a function to bridge the applications of web based information system in the environment of Diponegoro University so that the users simply remembers only one information of login to access all of the available applications. Hence, in the development of this SSO portal, the first functionality will be divided based on the group of the users that will access this portal. The group of the users is presented as follows:

1) Administrator
2) Common Users (for example lecturers and official employees)

Meanwhile, the second functionality is addressed by outlining the functions that will have SSO portal as the application organizer in the environment of Diponegoro University.

From the identification of the functionalities previously outlined, the modeling framework of the functional user administrator and the common users is presented using *use case diagram* (Fig.7).

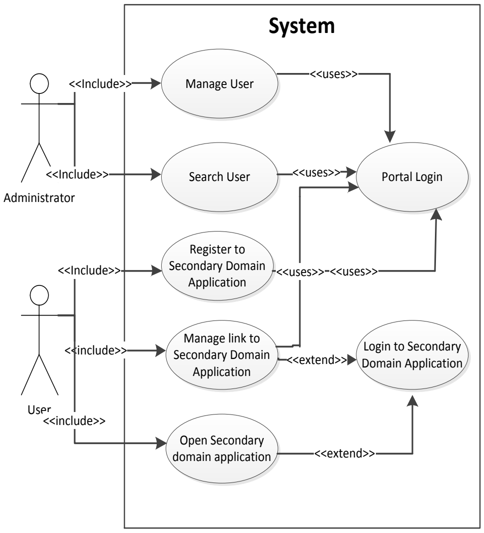


Fig. 7 - *Use Case Diagram*

3.3 The Design of Auto login Process

Auto-login process begins from a user demand to open the application stimulated when the user clicks the application menu. When the menu has been clicked, the validation of the registration for the login user information will be performed. Once it is complete rightly and properly, the SSO portal will do the hidden background process to open and fill in the form of application login with the login information that has been registered by the user. Subsequently, the portal will show the web frame containing the application opened by the user.

The explanation of the process above can be modeled in the flowchart in Fig 8 as follows:

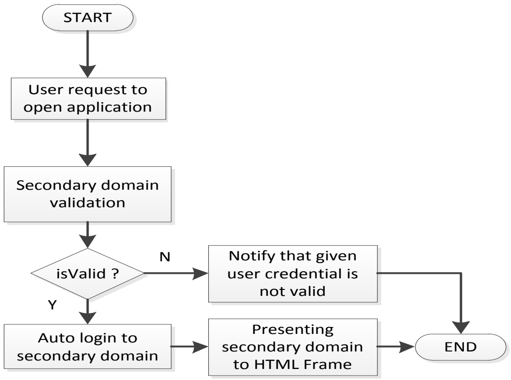

START
User request to open application
Secondary domain validation
isValid ?
N
Notify that given user credential is not valid
Y
Auto login to secondary domain
Presenting secondary domain to HTML Frame
END

Fig. 8 – Process of Portal SSO Auto login

3.4 Design of Auto logout Process

Other function that has been identified for SSO portal is by automatically logging out the application when the user signs out from the application of SSO portal and then stimulates the function. When logging out, SSO portal will call the logout links of each application managed y the portal. Then, through the portal, it will make a hidden interface that will do a hidden process to logout each application.

The process illustrated above will be shown in Fig.9 below

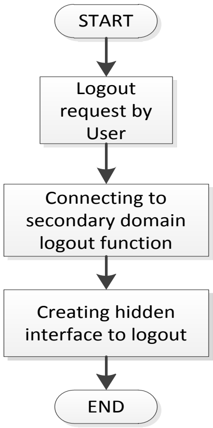

START
Logout request by User
Connecting to secondary domain logout function
Creating hidden interface to logout
END

Fig.9 - Auto logout Process

4. Presentation Integration

4.1 Managing Secondary Domain Application

As explained previously, a user is able to select the application in secondary domain application through the control panel provided in SSO portal in accordance with the right to use the application.

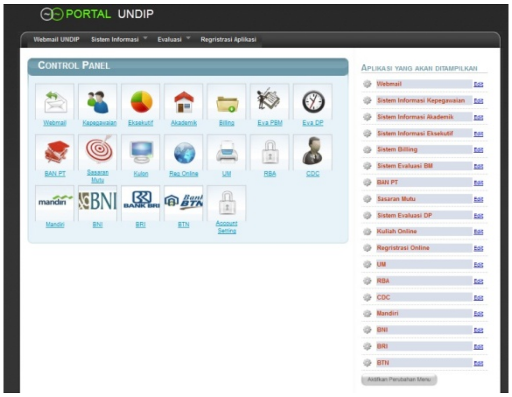


Fig.10 – User Control Panel

To be able to use the application, the user must save the information base by doing a registration in order to be able to access the applications managed by SSO portal.

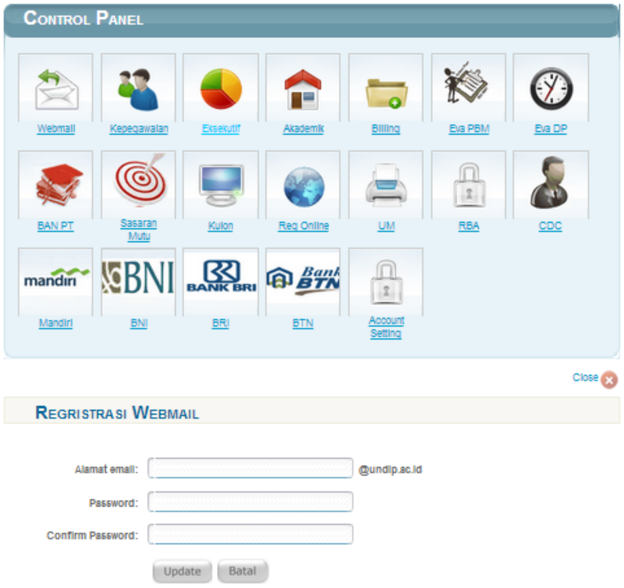
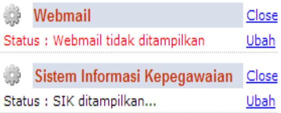


Fig.11 – Sample of Application Registration

Fig11 provides a sample of application registration in the portal in this case the webmail of Diponegoro University. The user here must give the webmail address and password before confirming and saving the passwords.



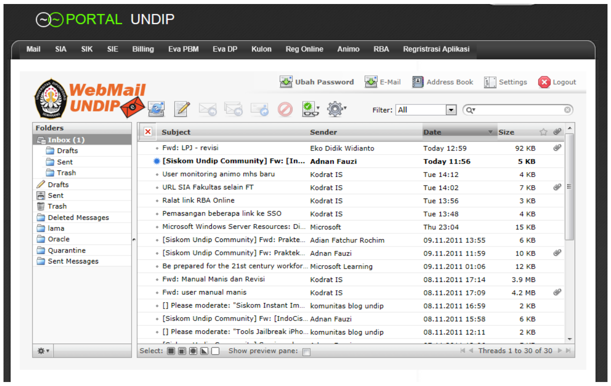
Webmail	Close
Status : Webmail tidak ditampilkan	Ubah
Sistem Informasi Kepegawaian	Close
Status : SIK ditampilkan...	Ubah

Fig.12 – Displaying the application on menu bar

Fig.12 above furthermore shows the way to display the application on the navigation menu of SSO portal. It begins by clicking the edit button on the right side of application that will be displayed. If the status of the application shows that the application is not displayed, the user can display the application by pressing the *change* button. Once the status of the application has turned into *application is displayed*, then clicking the activation of the menu change in the lower part of application list.

4.2 Secondary Domain Application in Portal SSO Frame

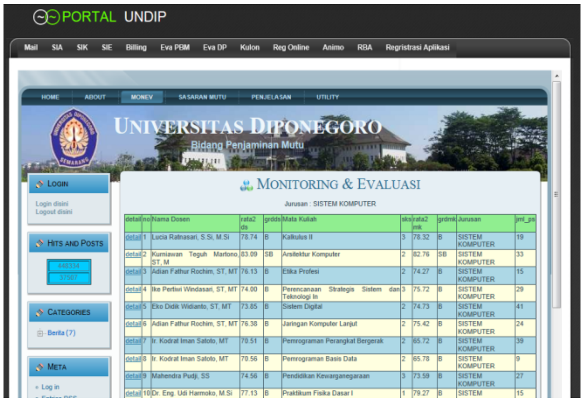
To register at the presentation level, SSO portal uses HTML Frame to display the secondary domain application. This domain application will display if the user information base for the intended application is valid. Fig.13 below is a sample of how the presentation of integration webmail application in SSO portal will be.



Subject	Sender	Date	Size
Fwd: LPJ - revisi	Eko Didik Widianto	Today 12:59	92 KB
[Siskom Undip Community] Fw: [In...	Adnan Fauzi	Today 11:56	5 KB
User monitoring animo mhs baru	Kodrat IS	Tue 14:12	4 KB
URL SIA Fakultas selain FT	Kodrat IS	Tue 14:02	7 KB
Ralat link RBA Online	Kodrat IS	Tue 13:56	3 KB
Pemasangan beberapa link ke SSO	Kodrat IS	Tue 13:48	4 KB
Microsoft Windows Server Resources: Di...	Microsoft	Thu 23:04	15 KB
[Siskom Undip Community] Fwd: Prakte...	Adian Fatchur Rochim	09.11.2011 13:55	6 KB
[Siskom Undip Community] Fw: Praktek...	Adnan Fauzi	09.11.2011 11:59	10 KB
Be prepared for the 21st century workfor...	Microsoft Learning	09.11.2011 01:06	12 KB
Fwd: Manual Manis dan Revisi	Kodrat IS	08.11.2011 17:14	3.9 MB
Fwd: user manual manis	Kodrat IS	08.11.2011 17:09	4.2 MB
[] Please moderate: "Siskom Instant Im...	komunitas blog undip	08.11.2011 16:59	2 KB
[Siskom Undip Community] Fw: [IndoCis...	Adnan Fauzi	08.11.2011 15:58	6 KB
[] Please moderate: "Tools Jailbreak iPho...	komunitas blog undip	08.11.2011 12:11	2 KB

Fig.13 – Presentation Integration between Webmail Application and SSO Portal

Fig.14 presents another sample in presenting the secondary domain application system for the evaluation of a teaching-learning process.



PORTAL UNDIP
Mail SIA SIK SIE Billing Eva PBM Eva DP Kulon Reg Online Animo RBA Regristrasi Aplikasi
HOME ABOUT MONEV SASARAN MUTU PENJELASAN UTILITY
UNIVERSITAS DIPONEGORO
Bidang Penjaminan Mutu
LOGIN
Login disini
Logout disini
HITS AND POSTS
CATEGORIES
Berita (7)
META
Log in

MONITORING & EVALUASI

Jurusan : SISTEM KOMPUTER

detail	no	Nama Dosen	rata2 ds	grdds	Mata Kuliah	sks	rata2 mk	grdmk	Jurusan	jml_ps
detail	1	Lucia Ratnasari, S.Si, M.Si	78.74	B	Kalkulus II	3	78.32	B	SISTEM KOMPUTER	19
detail	2	Kurniawan Teguh Martono, ST, M	83.09	SB	Arsitektur Komputer	2	82.76	SB	SISTEM KOMPUTER	33
detail	3	Adian Fathur Rochim, ST, MT	76.13	B	Etika Profesi	2	74.27	B	SISTEM KOMPUTER	15
detail	4	Ike Pertiwi Windasari, ST, MT	74.00	B	Perencanaan Strategis Sistem dan Teknologi In	3	75.72	B	SISTEM KOMPUTER	29
detail	5	Eko Didik Widianto, ST, MT	73.85	B	Sistem Digital	2	74.73	B	SISTEM KOMPUTER	41
detail	6	Adian Fathur Rochim, ST, MT	76.38	B	Jaringan Komputer Lanjut	2	75.42	B	SISTEM KOMPUTER	24
detail	7	Ir. Kodrat Iman Satoto, MT	70.51	B	Pemrograman Perangkat Bergerak	2	65.72	B	SISTEM KOMPUTER	39
detail	8	Ir. Kodrat Iman Satoto, MT	70.56	B	Pemrograman Basis Data	2	65.78	B	SISTEM KOMPUTER	9
detail	9	Mahendra Pudji, SS	74.56	B	Pendidikan Kewarganegaraan	3	73.59	B	SISTEM KOMPUTER	27
detail	10	Dr. Eng. Udi Harmoko, M.Si	77.13	B	Praktikum Fisika Dasar I	1	79.27	B	SISTEM	15

Fig.14 – Presentation Integration between the System for Evaluation of Teaching-Learning Process and SSO portal

5. The Result of Function Test

The functional testing of SSO portal administrator as listed in Table 1 below shows the result of the test on the Administrator's functions available in the developed SSO portal.

Table 1 – The Functional Testing of Administrator of SSO Portal

Functions Tested	Expected Results	Results
Making the SSO portal of user by administrator	The login made can be used to enter the SSO portal	Successful
Deleting the SSO portal user by administrator	User deleted will be lost including the data of the user	Successful
Seeking the user of SSO portal by administrator	User fulfilling the criteria of searching will display in the table of searching result	Successful
Resetting user's Portal SSO by administrator	The SSO portal user is not able to enter using the old password and must enter using a new password.	Successful

Table 2 below shows the result of the test to the functions of the user existing in the developed Single Sign-On portal.

Table 2 – The Functional Test of User of SSO Portal

Functions Tested	Expected Results	Result
Registration for the application at secondary domain by the user of SSO portal	Information of login user SSO portal in secondary domain application is stored in database of SSO portal	Successful
Auto login to Secondary Domain application	After clicking the link of menu of secondary domain application, user of SSO portal is able to auto login to secondary domain application	Successful
Manage link menu secondary domain application that will be displayed in navigation menu	In Menu navigation, there will be a link to secondary domain application	Successful
Auto logout from primary domain	If logging out from SSO portal, it will automatically log out from all secondary domain application	Working in almost all secondary domain application except the application that use dynamic session key

6. Conclusions

From the result of the research on the development of single-sign-on portal of Diponegoro University, some conclusions are drawn as follows:

1) Using the approach of *indirectly* single-sign-on developed in portal SSO, the session variables of secondary domain application are still right running well under the session of SS portal.
2) Similarly, the destroy session variabel for each of application when logging out from SSO portal mostly can run well; thus enabling to destroy the session in the secondary domain application. However, for the application of e-learning using the content management system moodle, *destroy variabel session* cannot run well due to the influence of *dynamic session key* variable from moodle.
3) In view of the use of frame to do integration presentation, handling the scrolling in the frame is needed. It is caused by the dynamic content of secondary domain application that makes the frame size always be dynamic.

References

[1] Arul Princy.A, and Vairachilai.S, A Survey on Single Sign-On Mechanism for Multiple Service Authentications, International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 12, December 2013, pg.40 – 44
[2] CodeIgniter Developer Team, http://codeigniter.com/user_guide, EllisLab Inc, 2006-2011, accessed in March 2012
[3] Jean Jacob, and Mary John, Security Enhancement of Single Sign on Mechanism for Distributed Computer Networks, International Journal of Modern Engineering Research, Vol. 3, Issue. 3, May - June 2013 pp-1811-1814
[4] Keneth C. Laudon & Jane P. Laudon, Management Information System: Managing the Digital Firm, Seventh Edition, Prentice Hall, 2002, 208-210
[5] S. Preetha, and A. RATCHANA, and S. Subashree, and S.T. Santhanalakshmi, Single Sign On Mechanism With Enhanced Security, International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-3, March-2014
[6] Tariqh Rahim Soomro, and Abrar Hasnain Awan, Challenges and Future of Enterprise Application Integration, International Journal of Computer Applications (0975 – 8887), Volume 42– No.7, March 2012
[7] The Opengroup, Introduction to Single-Sign-On, http://www.opengroup.org/security/sso/sso_intro.htm, Retrieved January 2012
[8]William Tse, Enterprise Application Integration (EAI), http://www.cs.ucl.ac.uk/staff/ucacwxe/lectures/3C05-03-04/EAI.pdf, Retrieved November 2011

Rinta Kridalukmana – born in Semarang, Indonesia in 1977, he got his title as Computer Bachelor from Department of Information System in Stikubank Semarang in 2003 and Magister title from STEI ITB (School of Electrical Engineering and Informatics, Bandung Institute Technology) in 2007. At the moment, he is one of the members of Association for Computing Machinery and a lecturer at the Program of Computer System Engineering, Diponegoro University since 2011. The research field is in Information System, Mobile application and integration data.

Kodrat Iman Satoto born in Madiun Indonesia in 1963. He's got his bachelor and magister degree from Department of Electrical Engineering, Gadjah Mada University in 1991 and 2002, respectively. At the moment, he is a lecturer in Department of Electrical Engineering, Diponegoro University, Semarang since 1993. The research fields he elaborates include database, computer network, and technology and information system.