Advances in Social Science, Education and Humanities Research, volume 172
4th International Conference on Education, Management, Arts, Economics and Social Science (ICEMAESS 2017)

The Unified Identity Authentication Platform of University Information System Based on CAS

——Taking Library Information System as an Example

Zhang Haibo[1, a,*], Lin Peifa[1, b], Zhang Xiaomeng[2, c], Li Xiaoyan[1, d], Zhang Zekun[2, e]

[1]Library, Beijing Institute of Fashion Technology, Beijing, 100029, China

[2]Information Center, Beijing Institute of Fashion Technology, Beijing, 100029, China

[a]hbdmzhb@126.com, [b]peking99@bift.edu.cn, [c]2540944916@qq.com, [d]db301@163.com, [e]281323910@qq.com, [*]corresponding author

Keywords: University Information System; CAS; Unified Identity Authentication; Library Information System

Abstract. With the rapid development of informationization in colleges and universities, colleges and universities had established a lot of information systems. In order to use these systems to achieve single sign-on and unified authorization and certification, a unified information system platform for identity authentication platform need to be built. Based on the CAS technology, this paper took the library information system as an example, and studied how to realize the unified authentication in the information system of the university in the aspects of the unified identity authentication architecture, the deployment and implementation of the CAS, and had achieved application effect with good results in the practical application.

Introduction

With the rapid development of information technology in colleges and universities, various information systems in colleges and universities had been built, and the features of these systems are increasing powerful. When teachers and students use these different information systems, they require identifying separately and authorized for different identities, different identities corresponding to different operating privileges[1]. For teachers and students, the registration of different information systems require different accounts and passwords; for information managers, the management of multiple information systems, the difficulty and increased workload, and easily lead to data inconsistencies. Therefore, it is very important to establish a unified, perfect, secure, easy to manage, portable, extensible user identity management system of the campus network.

The university information portal system provides the integration of various resources such as information and application. It provides a single access point, singleness, integration and personalization of the integrated resource in the way of the basic characteristics of the portal. The Information portal could improve the efficiency of the use of network resources to a certain extent, solve the data barriers between systems, and solve the unified implementation, management, maintenance and personalized features as well, what is more information needs of the contradiction between the realization of the "unity" and " Personalized "needs[2].

One of the most important functions of the information portal system is to provide users with identity authentication mechanism, unified control of user access to system resources. A user just be required logging in the portal system and then he get an identity, when he need to access the campus network within a variety of application systems and information resources, such as office systems, college news, mail systems, educational systems.

Therefore, the universal user management system, authorization management and identity authentication system are constructed based on directory services and certification services, that could make the organization of information and user's information to unified storage, and have hierarchical authorization and centralized identity authentication, and standardize the user

authentication method of the application system. Thereby, these can enhance the security of the information system and the convenience of the user to use, so that to achieve all the application of single sign possible[3].

This article combined with the actual situation of our school of information system, and took the book information system as an example, using the CAS technology, has carried on the research to the realization of the unified identity authentication platform of the university information system, and realized the unified identity authentication between the library information system and the school information portal.

CAS (Central Authentication Service) is an Open Source Project launched by Yale University to provide a reliable single sign-on method for Web applications. It is a set of Web-based implementation of SSO (Single Sign On) open source services. The purpose is to by through a common authentication system to manage and verify the identity of the user that distributes in an integrated system within the different heterogeneous systems of authentication work together. Users who are authenticated on the CAS will receive a certificate issued by the user who can freely access the system on each system that acknowledges the certificate and does not need to log in again[4].

The CAS contains the two parts of CAS Server and CAS Client. CAS Server is responsible for the user's certification work that requires being deployed independently. What is more, CAS Client is responsible for handling the requested resource of the protected about the client's that needs to redirect to the CAS Server when log in[5].

Background and Demand Analysis

Unified identity authentication is one of the important contents of the university information integration. It can solve these problems: First, it can solve the problem that a user n need to use multiple accounts and passwords when he want to log in different systems. The second is to solve their own systems have a set of certification and user management mechanism what is not conducive to unified management issues. Last that someone discharge from school is able to still log on some of the school business systems to result in management loopholes due to the lack of unified management.

Unified identity authentication platform system is a centralized user authentication management and integration environment, the system can accomplish all the information system users identity management and authentication. On the one hand that to facilitate the use and management, on the other hand also to ensure the advanced nature of the entire system and safety.

Modem Electronic Library Information and Nets System (MELINETS), which is a library information system of Beijing Chuangxun Software Technology Co., Ltd is applied our library information system. The entire system consists of three parts: (1) Library Business Application: ① Interview Subsystem; ② Collection Circulation Subsystem; ③ Continuous Publication Subsystem; ④ Public Search Subsystem. (2) Regional Resource Cooperation and Sharing Application System: ① Z39.50 Public Search Subsystem; ② Inter-library Loan Sub-system; ③ Catalog Center Subsystem. (3) Administrative Business Management System:①Personnel Management Subsystem; ② Equipment Management Subsystem [6].

MELINETS uses C/S or B/S application server/database server architecture and adopts various languages such as POWERBUILDER, JAVA, C. What is more, database platform uses large relational database management system what is able to support SYBASE, ORACLE and other databases to develop and enhance sexuality and stability. Server-side equipment is made of using super microcomputer, dedicated server and small and medium computer. The operating system is so suitable for large, medium and small types of libraries and information Center that is made of using UNIX, PCUNIX, LINUX, WIN2000 / 2008/2012[6].

The basic requirements of Library Information System that is acceded to university unified identity authentication platform:

(a) The integration of identity authentication of library information system includes teaching staff users and all students in the school.

(b) After the integration of the library information system, the user (students, teachers) can

achieve a single point of landing from the information portal. That is, when a user has logged in information portal, no need to open the library information system login interface and enter the library information system user name and password, he can be directly into the book Information system or specific business processing page.

(c) To retain the original login entry of library information system to prevent a unified identity or information portal system problems, or the library information system not being used normally.

(d) Student user login is used for both system matching key field for student number. Teacher user login is used for both system matching key field for job number.

(e) The university information portal platform provides users with a unified access to the library information system. A user enters the library information system without having to enter the user name and password directly to access the library information system after click on chain (the integrated address of the authentication).

System Architecture Analysis

In this paper, the authentication between the library information system and unified identity authentication center platform is to achieve the teacher and student users log in the school information portal. And they can jump to the library information system without need for the certification.

The unified identity authentication architecture and processes, for library information system as an example (Figure 1).

In general, CAS contains two parts: CAS Server and CAS Client, and they require to be deployed independently. The CAS Server in this paper is the unified identity authentication center platform in Figure 1, which is mainly responsible for the user's authentication. The CAS Client in this paper is the library information system in Figure 1, which handles the access request to the client's protected resource when redirected to the CAS Server.

In figure 1, information portal and unified identity authentication center share center database, and library information system has its own database. Center database provide teacher and student information to library database through the data exchange. Thus, this can ensure that the data of the teacher and student information are the same in the two databases. The information of the teacher staff generally includes the employee's job number, name, department number, department name, duty, title, age, gender and other information; student information generally includes student number, name, department, class, student category (undergraduate, graduate, adult students, returned students), age, gender and other information.

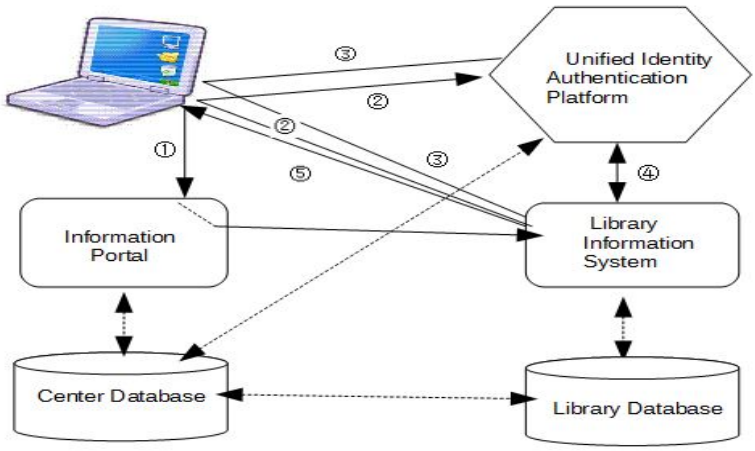

Figure 1. Unified identity authentication architecture and processes

In figure 1, Library Information System and unified identity authentication generally include 5 steps of authentication procedure.

① Teachers and students send access to the library information system request through the information portal by computer or mobile phone and other clients. The domain name is assumed

for http://tsg.university.edu.cn:8080/. Library information system takes the local call ID "JSESSION" by browser.

② If the ID does not exist, then redirected to unified identity authentication center, carry address, trigger request http://cas.universtiey.edu.cn/?service=http://tsg.universtiey.edu.cn:8080/. (The domain name of unified identity authentication center is assumed for http://cas.university.edu.cn/)

③ The unify identity authentication center takes the global session ID: "CASTGC" by browser. Ticket Granted Cookie (TGC). If the ID does not exist , the user can enter the login page. After the user has logged in, a global session TGT (Ticket Granting Ticket) is produced, and then the authentication is redirected to the library information system, and carry the verification ticket ST (Service Ticket), http: //tsg.university.edu.cn:8080/?ticket=ST-XXX-XXXX. If the ID exists, then the authentication directly orients to the library information system.

④ The library information system gets the ticket from the browser address bar, and then sends it to the unified identity authentication center. The unified identity authentication center verifies the ticket's legitimate legal, and then returns the user login information to the library information system, what creates a local session locally.

⑤ Library information system achieves the local session, and then sends to the user's computer. The computer obtains the global session ID: CASTGC and local session ID: JSESSION.

Deploying of System

Deploying the Server-Side. The unified identity authentication center platform, which is the CAS Server, is a set of Java-based services, this service is deployed as a Java Web Application on a Web server that is compatible with the servlet2.3, in addition, because the interaction between the Client and the CAS Server uses the Https protocol, the servers that deploy the CAS Server also need to support the SSL (Secure Socket Layer) protocol.

Deploying a complete CAS Server on Tomcat mainly follows the following steps:

Configure Tomcat to Use the Https Protocol. Tomcat supports Https, the main job is to configure the SSL protocol. SSL can protect the data transmission on the Internet security. It uses data encryption technology to ensure that the data transmission in the network in order that the data will not be intercepted and eavesdropping. It has been widely used for identity authentication and encrypted data transfer between Web browsers and servers[7].

Deploying the CAS Server. The CAS server is a Web application package that will download the file to tomcat's webapps directory and rename it to "cas.war". Restart tomcat, if you visit https://cas.university.edu.cn/cas, a normal CAS login page, it will show "CAS Server has been deployed successfully".

Although the CAS server has been deployed successfully, but this is only the basic system operation. In actual use, it also needs to be done to extend and customize according to the actual profile, which the most important is to expand the authentication interface and the CAS server interface.

Extended Authentication Interface. The CAS server completes the authentication of the user by processing the credential information of the logged-on user (such as the username / password). It may need to retrieve a user account information to the database, may also retrieve the username / password in the XML file, and possibly through the LDAP server, and so on. In this case, CAS provides a flexible but unified interface and implementation of the separation of the way. In this paper, the actual application of the database to retrieve a user account information. So in Figure 1, the teacher and student's information data exchange of the center database and the library database is a prerequisite for the realization of unified identity authentication.

Authentication Method of JDBC. JDBC (Java DataBase Connectivity) is a Java API for executing SQL statements. It provides unified access to multiple relational databases, and is consisted of a set of classes and interfaces written in the Java language. JDBC provides a benchmark, so we can build more advanced tools and interfaces, so that database developers can write database applications.

The authentication information of teacher and student user is usually stored in the center

database. CAS software provides a JDBC connection through the database to verify the default implementation. Based on this package support, we only need to do some configuration work to achieve JDBC certification.

Interface Customization. CAS provides a set of default pages in the directory “cas / WEB-INF / view / jsp / default”. Before deploying CAS, we may need to customize a new set of CAS Server pages to add some personalized content. The easiest way is to copy a default file to the "cas / WEB-INF / view / jsp" directory.

Deploying of the Client-Side. The library information system, is the CAS Client in this article. The purpose of single sign-on is to allow multiple applications associated with the same login process, this paper in the process of constructing two simple applications, respectively casTest1 and casTest2 as an example. They have only one page, showing the welcome message and the current login user name. These two applications use the same set of login information, and only registered users can access, through the configuration of this article, to achieve single sign-on, that is, just log on once you can access the two applications.

Establish Trust with CAS Server. Assuming that the server is deployed separately on a machine A and the client application is deployed on machine B, since the client application communicates with the server using SSL, it is necessary to establish a trust relationship between A and B's JRE(Java Runtime Environment). A machine need to generate B machine’s certificate and configure Tomcat's SSL protocol. In the last, we also need to add A to the B's trust store.

Configure CAS Filter. In the library information system, we copy the corresponding file to “WEB-INF / lib” directory, modify the web.xml file, and add CAS Filter. After the completion of all access to meet “/ protected-pattern / “ specify the path of resources, are required to the server identity authentication center login, if the need to be protected “casTest1”, we can specify “url-pattern” as "/ *".

Pass the Login User Name. If a user log in CAS success, the browser will return the Cookie, and set a new Service Ticket. The client application has every session. The CAS Client's Filter has been handled. After the success of the login, the CAS client can directly from the session attribute to obtain the current login user's user name.

Conclusion

Aiming at the independent information system of colleges and universities, the unified authentication between information systems can effectively solve the single sign-on problem of teachers and students, and also help the information management personnel to manage and maintain the information system. This paper has used the CAS technology and taken library information system as an example, studied and discussed the unified identity authentication technology of university information system. In practical application, it had obtained a better application effect.

Acknowledgment

The work described in this article was supported by grants from the Teaching Reform Key Project of Beijing Institute of Fashion Technology (No. ZDJG-1510) and the Science and Technology General project of Beijing Municipal Commission of Education (No.AJ2016-11).

Reference

[1] Hong Chen, Research and Realization of Digital Campus Uniform Identity Authentication System[D]. University of Electronic Science and Technology of China Master’s Thesis, 2013. (in Chinese)

[2] Jie Ma, Research and Implementation of University Information Portal User Management[D], South China University of Technology Master’s Thesis, 2010. (in Chinese)

[3] Zhijun Ding, Construction of Data Center Platform of Digital Campus in Universities[D], Fudan University Master's Thesis, 2009. (in Chinese)

[4] Yi Qin, Single Sign-on Based on CAS and Integrated Management in the Digital Library Portal[D], Beijing University of Posts and Telecommunications Master's Thesis, 2009. (in Chinese)

[5] Yingjing Huang, Application and Design of SSO in Digital Campus Systems Based on CAS Protocol[D], South China University of Technology Master's Thesis, 2012. (in Chinese)

[6] Jiwen Gong, Sciencepaper Online http://www.paper.edu.cn/releasepaper/content/200606-487. (in Chinese)

[7] Jazib Frahim, Qiang Huang works, Ji Wang, Jinwen Luo, FanBai translates. SSL Remote Access VPNs[M], Posts & Telecom Press,2009. (in Chinese)