A Method and Tool for Integration and Concentrated Control of Authentication Process in organizational Software Systems (Case Study and Implementation in Sarmayeh Bank of Iran)

1Mahdi Shabani, 2Ali Torabi, 3Amin Shateri

1Master Degree of Software Engineering Payame Noor University, PO BOX: 19395-3697, Tehran, IRAN
2Bachelor Degree in Hardware Engineering President of Sarmayeh Bank Information Office, Tehran, IRAN
3Bachelor Degree in Hardware Engineering Master official of Linux Professional Institute (LPI)

ABSTRACT

Nowadays, with increasing the influence of information technology in organizations have an appropriate infrastructure and well-defined in organization, is fundamentally necessary for the purpose of integration of key processes like single sign-on authentication (SSO) and unitize the organization's information assets. Availability such infrastructure maintains appropriate level of integrity and independence of logical systems interaction, meanwhile will prevent of forming island systems in the enterprise architecture and reduce the costs and risks and causes of centralized access control. However, implementing of single sign-on in enterprises is one of the most complicated forms of integration in organizations as a result of they include integrative several system and heterogeneous approach sometimes also has been deployed on multiple platforms and is managed heterogeneous access schemes. In this paper we explain the requirements and challenges of single sign-on implementation mechanisms also pay attention to the technologies in the applications in Iranian organizations, especially banks and financial institutions and credit, has been presented a methodology and tool for integration and Central Control authentication process in enterprise systems with using LDAP and CAS server. The proposed method has been implemented and operated in headquarters and 150 branches of Sarmayeh Bank of Iran for over 15 applications and 1600 users of the whole country. The achievements and challenges which organizations are facing in the movement toward integration a long with used strategies to overcome these obstacles in Sarmayeh Bank is presented in the results section.

Key words: Integration, Single Sign On (SSO), Light Weight Directory Access Protocol (LDAP), Central Authentication Service (CAS), Certificate Authority (CA), Public Key Infrastructure (PKI)

Introduction

IT has influenced on organizations in today's world and presence of an appropriate platform for integration of key processes like authentication and unification of organizational information assets is an essential affair. Such a platform not only maintains a favorable level of integration and independence for systems but also it prevents from formation of island systems phenomenon in organization and reduces organizational risks and costs.

In Information Technology Enterprise Architecture (IA) and base pattern which is used for it (Enterprise Architecture Model, figure1) systems integration and software services are of great importance and are more applicable to layers "ITC" and "applied systems". In this model, each layer serves its upper layer and determines its lower layer requirements.

On the other hand, development of applied software in new model which has started from 2001 and 2002 and makes use of business process management systems (BPMS) tools, has formed a new pattern for integration based on utilization of common platform services. In the next steps, development trend of organizational applications in 2000 decade is reviewed with emergence of component-based approaches in software engineering. Many services which were formerly considered as internal software of other applications are now considered as independent. At the present time, integration concept has changed a lot with such services and their place in applied software architecture and figure(2) indicates future direction of enterprise applications (simplified) [1].
Therefore, platform concept is being developed in applications architecture and contains more and more layers and components. The influence of this trend and specialization of the market of these platform components is such that even the largest sellers of enterprise applications (ERP) plan for transformation of their applications architecture to component-based architecture. For example, architecture of ERP applications which are provided by SAP and Oracle (leaders of ERP market) indicate a competition on incorporation of more and more components of platform services and integration in their products [2]. Large Iranian organizations and especially public institutes and banks and credit organizations have to use external organizational resources especially in IT due to their activities nature. Therefore, central authentication system (SSO) can be as one of the necessary characteristics and the first step in integration process of enterprise applications.

In this paper, mechanisms and tools of implementation of a SSO platform is reviewed and then, a method for integration and concentrated control of the process of authentication of various software systems is provided using CAS and LDAP servers. Finally, a successful sample of implementation of the proposed method is provided. This sample was implemented in the headquarters and 150 branches of Sarmayeh Bank in Iran and for 15 applications with 1600 users along and is accompanied by challenges ahead of enterprises in integration process.

**Fig. 1: Enterprise architecture model NIST [1]**

**Fig. 2: Sample architecture of enterprise applications in future[1]**

2. **Definitions, necessities and advantages of SSO implementation:**

Definition: SSO is a mechanism through which one single authentication action is conducted for identification of users and users are allowed to access other systems and software, without necessity to enter various passwords.

Users must clarify their identification in all software applications and systems in organizations for using specialized service. General mechanism of authentication is based upon user name and password which is also used in most application software in organizations. This enables service providers to make service exclusive. It is obvious that we face two cases when the number of systems increases:
1. Individuals use one single user name and password for all services.  
2. Individuals have to remember one username and password for using each system.  
   In the first case, if there is no suitable implementation for security system, user's security will be endangered in all other systems when hackers become aware of username and password of that system. In the second case, user has to remember many different usernames and passwords which are very difficult for most users and usually software impose various rules for setting the length and shape of passwords. Therefore, users have to store information in unsafe places in order to be able to remember passwords and this is of course a great threat for ITC platform.
   If appropriate solutions are not provided for this, users will face the problem of having many usernames and passwords. Therefore, the following hints can be proposed to justify the necessity of conducting the present research:
   - Rapid responding to information needs through organizing databases and users' profiles with the aim of maximization of accessibility, doing changes and reporting
   - Facilitation of problem-solving and presentation of organizational solutions through minimization of additional works among different sections' plans
   - Convergence and integration of subsidiary organizations and contractors information
   - Creation of equilibrium between information accessibility and information security
   - Increasing human factors productivity in organization
   On the other hand, implementation of this system in an organization has many advantages for users of different systems:
   - Facilitation of data flow inside and outside of organization
   - Facilitation of integrated authentication through a concentrated input port and access to various software which are used in organization
   - Preparation of a standard and development document and design of a mechanism for authentication of systems within the framework of enterprise architecture document
   - Lack of increase in the number of user codes and passwords for users and lack of need to changing password in repetitive form in all systems and reduction of time and costs related to password recovery mechanisms
   - Increase in level of security of access to systems and software in all sections like: entrance, exit, changing password and …
   - Facilitation of formation of mechanism of integrating central authentication system with enterprise public key infrastructure(PKI)
   - Technical supporting, management and easy control of users of systems and software
   - Making sure that the IT infrastructure supports access to organizational goals and will be active with fast advance of technologies

3. Authentication mechanism based on central authentication service (CAS):

   Implementation of a central authentication system in an organization contains one of the most complicated forms of integration because the mentioned mechanism contains several system and approach which are established usually on different platforms and are inhomogeneous. In SSO mechanism, single sign-on for user identification will be implemented in an integrated way while each system will take responsibility of authentication control in an independent way.
   Considering all advantages and complicated aspects, selection of solution is one of the most important aspects of platform operation. Implementation of special and non-standard solutions in large organizations do not seem to have a good prospect and studies show that such solutions are not comprehensive and cannot be developed well [3]. Risks like inappropriate analysis, lack of support for software in the framework of development of platforms and lack of documents will cause problems for contractors and IT partners of the organization. In spite of this, many standardized approaches have been proposed in the last few years which are mainly developed in academic environments in the form of study plans and after receiving appropriate feedback, they have become appropriate frameworks.
   Solutions which have been proposed for covering these requirements and have been standardized in implementation of Enterprise-Single Sign-on generally follow similar architectures which are based upon establishment of key components. One of the most important components which play role in management of users' authentication based on identification is "central authentication service (CAS)" which acts as user interface authentication service.
   CAS can solve the mentioned problem with an easy method and is able to solve the problems of integration in the process of authentication with focusing on this layer in all services and separation of users' access control. Authentication layer is a section which is used in all services and each service and product has a special implementation of this. If we are able to present a secure implementation of authentication and this authentication is web-based, it is enough to select a service or gateway as reference and refer all authentication requests of organizational services to this center and receive the result of authentication in this center. This is a simple general schema of mechanisms like CAS, JOSSO and OpenSSO[3]. CAS protocol proposes the closest possible mechanism of implementation to satisfy organizational needs and operational requirements.
This mechanism presents a wider spectrum of software interfaces in inhomogeneous technologies and has a great flexibility in establishment of systems supporting.

CAS protocol is made up of 4 working units: “client web browser”, “web application requesting authentication”, “CAS server” and “authentication servers” [4]. Generally, all applied services play service-receiver role of CAS in general architecture. One of the advantages of this protocol is lack of requirement to a component which can be installed on user web browser. This layer is the simplest level of protocol architecture.

Services integration is carried out through CAS client. This process is called Casifying and includes changing the layer of authentication in applied services. CAS protocol has presented components for .Net, Java, PHP, and also modules for web servers like: Apache and IIS. CAS protocol does not use mechanism of cookie sharing contrary to many other solutions. An alternative solution is production of a session ID which after authentication in the first layer (web browser) allows a user to access services. This session ID is only valid in the level of CAS server and in common forms and is called TGT. According to this session ID, a disposable user identity license is produced and is traded between client browser and CAS server using master-key. This mechanism reduces the possibility of man-in-the-middle attacks in session and provides a high level of security in the process of users' authentication in the level of applied services. After successful authentication of user, user's general session is produced according to TGT. If user requests service and if TGT is valid, one ST or service-ticket is produced. After that, this ticket is validated while it is only used for user access to a special service. [5]

CAS server has the responsibility of relationship with data resource needed for users' authentication based on user letter of credit. This data resource can be databases, LDAP servers or reserve of X509 Certificate. Furthermore, CAS server can support methods based on proxy as one of the most complicated forms of authentication and also it has a limited support of SAML in 2.0 version of CAS protocol has been predicted which is used for development of schema related to users' information characteristics and implementation of Single Sign Out capability. Furthermore, possibility of supporting Open ID protocol also exists [6]. Figure (3) indicates the schematic of the described process.

4. Reasons for selecting CAS protocol:

- Presentation of a comprehensive solution for central authentication or Single Sign-on
- Implementation of concentrated input point to all services
- Possibility of authentication of certificate presented by user against a wide range of servers
- Implementation of authentication method based on service using delegated authentication
- Capability of development of information schematic of user's presence based on SAML standard and possibility of presenting unique alternative ID for each service instead of common user name
- High flexibility in web-based authentication cycle
- Possibility of using audit and comprehensive events registry
- Support for a wide range of technologies and executive platforms and simplicity in integration
- Presentation of a comprehensive and simple solution for management services
- High accessibility and development capability

![Fig. 3: Schematic of authentication mechanism in CAS protocol](image-url)
- Open-source structure and free license for exploitation

5. Case study and implementation in Sarmayeh Bank of Iran:

Researchers asked permission from the Sarmayeh Bank management and tried to investigate and analyze application software condition in the Bank in relation to authentication and implementation of the proposed plan in order to reach IT architecture goal of Sarmayeh Bank. Primary results of recognition phase indicated that Sarmayeh Bank is not resistant against this problem and as use of applications increases, users face the problem of numerous passwords and usernames in different applications. In the timeframe of this research, about 20 applications were active in the bank and each employee had several usernames and passwords dependent on his/her organizational position (staff/branch) [7]. Considering special complications of execution of integration projects and novelty of the concept in internal organizations and low experience in implementation of such projects and also development of trend of use of web application in bank and in order to reduce risk of execution of plan which is resulted from systems operation, the project was divided into two phases:

First phase: implementation of an integrated infrastructure for single sign-on (SSO) for web application: in this phase, definition and implementation of a standard for integration of a faster and more certain authentication is achievable due to coordination of the used technologies in implementation of web application and it is considered as Web Single Sign-On (WSSO). Therefore, the Bank's organizational portal was determined as system users' login and authentication was conducted based on this mechanism and in one step and user can use services and information of other applications according to access rights after login and being authenticated, without need to re-authentication and re-login in each them.

Second phase: development of influence domain of the defined integration standards in the first phase to other bank application: in this phase, authentication section of other application is developed according to the prepared standard of authentication layer so that this mechanism can be used and it is considered as enterprise single sign-on (ESSO). In this phase, integration of SSO infrastructure can also be investigated enterprise public key infrastructure (PKI). Figure (4) shows architecture of SSO infrastructure components which has been implemented.

![Fig. 4: architecture of SSO infrastructure components](image)

6. Steps and key activities of plan implementation

This project was implemented in 6 steps as follows:

6-1-recognition, analysis and planning: in this step, activities of planning, recognition and problem analysis were conducted in order to prepare work breakdown structure (WBS) and SSO architecture plan. Furthermore, determination of executive team and duties and road map clarification and identification of transferable systems on this platform were carried out in this step.

6-2-launching and development of infrastructure: in this step, LDAP server was launched and configured as background service in order to authentication and maintenance of users' information in the network. 27 standard identification characteristics were added to standard characteristics
set of LDAP in order to develop users’ profile information domain.

6-3- presentation of advice and education service to contractors: in this step, necessary actions were taken in order to implement the plan in experimental and operational environment and performance test.

6-4- integration of authentication services with public-key infrastructure (PKI) of bank: integration of authentication services with public-key infrastructure (PKI) of bank for internal/external users was conducted in this step.

6-5- created of an automatic mechanism for password recovery: in this step, with using a set of web services to communicate between SSO infrastructure and Active Directory server, made possible to change and recovery password by users through the enterprise portal. Security issues have been considered in the process. Mechanism of changes password is through the web-based enterprise portal and mechanism of password recovery using valid profile information and bank's relationship infrastructure with Telecommunication Company of Iran implemented. So that password recovery process was conducted through receiving verification message and new password message (in two steps) in users mobile.

6-6- transfer and operation: in this step, after launching the infrastructure, password integration policies and transfer of user accounts information to Active Directory was implemented and each of contractors carried out the process of adjustment their software with supervision of executor. Over one year after launching the service of authentication mechanism (SSO) in Sarmayeh bank, more than 15 application were transferred to this platform and authentication layer them with this standard were operated.

Results:

In the present paper, necessity, advantages and challenges ahead of implementation of integration mechanisms especially integration of users’ authentication in SSO form in organizations, a method and tool was proposed for integration and concentrated control of the process of authentication of different software applications using LDAP and CAS servers. The proposed method was implemented in Sarmayeh Bank of Iran for over 15 applications with capability of automatic password recovery through mobile message. Furthermore, functions of this infrastructure were developed and it was improved up to a "users' management" service with development of users' profile characteristics to 27 characteristics and formulation of system trends for on-time updating of personnel changes in information repository Sarmayeh bank. Considering the created platform in Sarmayeh Bank, integration of information systems and operational services of subsidiary companies and commercial partners which is called "B2B integration" or "integration" was facilitated.

On the other hand, transformations in the field of business models (like out-sourcing, shrinkage, horizontal separation, e-commerce, virtual organizations and so on) and in the technical subject (like internet, intranet, web, mobile networks and so on) over the past few years have made organizations to cooperate with each other and integration mechanisms like the proposed method in this paper can be effective and helpful and it can be used in other organizations as the first step in integration.

References