

GateKeeper

An Enterprise Identity Management System (EIMS)

1 Executive Summary

Organizations manage their operations starting from adopting heterogeneous operating systems evolving towards adopting heterogeneous applications. With heterogeneous infrastructure, organization starts using Microsoft Windows, Unix and Linux operating systems altogether running office works. At the same time, applications to support organizational operations grow. As a result, organizations normally need Human Resource Management System, Financial Information System, Workgroup Portal and so on. These heterogeneous applications become the heart of organizations to manage operations thus generating income from them.

However, with the growth of heterogeneous applications, operational risks attributed to users and system administrators increase. Besides that, there are also inherent network security risks. For example, using relational database or LDAP (Lightweight Directory Access Protocol) database as authentication repositories is not very secure because of passing passwords around. Apart from that, organizations need to be able to perform cross application functionalities to reap most from investment in the existing heterogeneous applications. These cross application functionalities are: cross application login (single sign on), cross application access level, cross application auditing, cross application profile synchronization, cross application user provisioning, cross application service provisioning and cross application organization knowledge. With these cross application functionalities, organizations equip themselves to be more efficient, productive, effective, and competitive.

We develop an Enterprise Identity Management System (EIMS) to address problems related to increase operational risks and to provide the cross application functionalities in heterogeneous applications' environment. EIMS is also well-known as an identity and access management solution. The EIMS solution is called *GateKeeper*. Gatekeeper has been deployed University Malaya (UM), Malaysia to manage 33,000 users in the environment of heterogeneous applications. In UM, Gatekeeper is known as Central Authentication Management System (CAMS). CAMS won an innovation award in Anugerah Inovasi Penyelidikan Bersama Antara Sektor Awam Dengan Sektor Swasta Tahun 2006 (AIPB 2006).

2 Organization Challenges

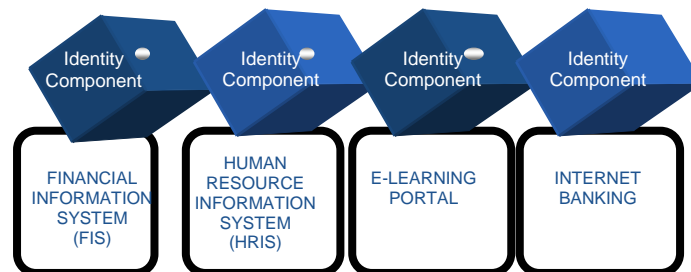


Figure 1: Identity Components in Applications



Almost all applications running within organizations have identity components. The identity component is used for authentication and authorization. Authorization deals with access levels within applications. With heterogeneous applications depicted in

Figure 1, the problems below will arise

- Increase operational risks
- Increase network security risk
- Inability to perform cross application functionalities

2.1 The Diversity of Access Methods is a Source of Operational Risk

System Administrator	End Users	Network Security	Database/LDAP -based authentication
<ul style="list-style-type: none"> - Multiple passwords give chances to fraud - Manage multiple user repositories waste productivities - Spend much time entertaining end users for profiles not up to date 	<ul style="list-style-type: none"> - Remembering various passwords becomes cumbersome with increasing applications - Synchronizing profiles between systems is waste of productivity - Multiple passwords give chances to fraud (e.g. group password) 	<ul style="list-style-type: none"> - Mixed of high and low security of application servers may compromise overall security - Low security applications are a weak point to penetrate the whole network. 	<ul style="list-style-type: none"> - Passwords are passed around for comparison and matching during authentication - Risk of passwords interceptions - Passwords hashings are still breakable
Less Productive	Increase Operational Risk	Compromise overall security	Passwords passing around

2.2 User information are not synchronized in each application

As an organization grows, departments and divisions are created with their own internal systems. Each application will have its own user repositories. Separate user repositories have high risk of different user information on a same user. It is reported in some cases, a staff may be reported an HR system, but not in a Financial System. As a result, the staff cannot get his or her paycheck in three months.

2.3 Inability for Tracking & Auditing User Transactions that across many applications

When users access applications, unauthorized data creations, modifications and deletions are possible without proper authorization. With heterogeneous applications, getting consolidated view of user activities in all applications will be very difficult, and may take long time. Failure to get cross-application audit in short time may impose severe penalty for any hazardous user activities.

2.4 Service Provisions for cross application is difficult

To have a special group that have an aggregate service of many applications is difficult. For example, in a university, we want to have a special group to have a special tuition rate and special grade monitoring.

With two separate applications managing tuition rate and managing grades, managing this special group is difficult because synchronization of profiles and access needs to be done at the both end of the applications.

2.5 Difficulty to register and to archive thousands of users across many applications

In an organization with thousands of users with heterogeneous applications, registering new users and archiving old users will be very cumbersome. For example, in one of the prestigious university in Malaysia, each year, there will be about 5,000 students registering and graduating. With many applications attributed to each student such as Student Information System (SIS), Financial Information System (FIS), e-learning, student portal etc, the amount of work needed to register and to archive the users will be very cumbersome. This amount of work does not include other work involving for student suspension, cross-application access allocation and more.

2.6 A collective view of user information and activities across many applications is not possible

With many applications allocated for users, often, getting user information and user activities consolidated from all applications in real-time is not possible. For example, in a university, just by typing a student id, a lecturer may want to a get student profile from Student Information System (SIS), and at the same time, student activities consolidated from the e-learning application. This feature will be difficult because the same student may have different username in SIS and in the e-learning application.

3 Problems, Features, Benefits in a Nutshell

	Problems	Features	Benefits
1	<p>Organization:</p> <ul style="list-style-type: none"> - Repeat processes and resources of building identity for each applications, waste productive time - Inconsistent & Not Most Recent Users' Common Attributes (i.e address, phones etc) across applications - Organization cannot map organization structure and customer identity structure to every applications <p>Users:</p> <ul style="list-style-type: none"> - Needs to remember to many passwords that increase risks for impersonation and fraud 	<p>“Build Once” Identity Approach</p>	<p>System Owners</p> <ul style="list-style-type: none"> - Reduce operating cost by reduce wastage on resources and efforts. - Managing identity is shared and distributed across applications owner. - Transacting and tracking users with most updated and consistent data across applications - Organization can map organization structure and customer identity structure to every applications <p>Users:</p> <ul style="list-style-type: none"> - Need to remember one password with enforcement of a level of password strength
2.	Some applications may not have strong security defense	Appended Security on each layer that is performs internal encryptions test behaving as first line of defense	Increase applications security on top of existing internal security.
3.	Users: - Need to relogin for each access	Single Sign On	Users: - Seamless access after login once
4.	Organization cannot provide an aggregate online service from disparate applications.	Cross-Applications Service Provisions	Organization can provide an aggregate service than consists of online services from various applications
5.	Users: - Signup process to each application is painful.	“Only Once” User Provisioning	Users sign up only once. Organization



	<ul style="list-style-type: none"> - It may take days because of paper-based processes. <p>Organization</p> <ul style="list-style-type: none"> - many resources and verifications involved for signing users for each applications 		Resource and verification process reduced with paperless processes.
6.	User information are not structured logically or are not synchronized across applications	Synchronized and Transformation Services	All user data are logically sound and synchronize across applications
7.	<p>Preparing application audit report for standard compliance such as Sarbane/Oxley Compliance is painful after having islands of applications</p> <p>Any disruptive users' behaviors cannot be resolved in across all applications in intranet/environment because of no information provided on macro and micro level of users behaviour</p>	Cross-Application Audit Services	<p>Preparing report centrally is possible without having to manually inspect each application.</p> <p>Disruptive users behavior can be curbed and resolved from central.</p>
8.	Username/Password authentication does provide enough security	Multi-factor Authentication Ready	Organization can enforce user to authenticate with smartcard, MyKad, biometric etc after using username/password

4 Gatekeeper Packages

We have developed several gatekeeper packages to address the issues and the problems addressed before.

Packages	Features
Single Sign On	Consolidate Login for Web App, client-server, emulator (mainframe), OS windows, OS Linux
Cross-App Access Level	Consolidate Access for Web App, client-server, emulator (mainframe), OS windows, OS Linux
Cross-App Auditing	Consolidate Audit for Web App, client-server, emulator (mainframe), OS windows, OS Linux
Cross-App Provisioning	Consolidate User Provisioning such as Add new user, archive user for all apps etc
Cross-App SyncFormation	<p>Synchronize User Profiles among for Web App, client-server, emulator (mainframe), OS windows, OS Linux</p> <p>Consolidate user information from various applications to be viewed real-time.</p>
Authentication Type Synergy	Consolidate Authentication Type i.e. Biometric, MyKad, multi-factor etc

5 Cross-Application Login, Access & Service Provisioning

	User Experience	System Administrator Experience	Service Administrator Experience
Features	<p>Login once, access everywhere with restrictions</p> <p>A student updating address in student portal will be affected in Student Information System and Financial System</p>	<p>Manage users, groups, applications centrally instead of going to each applications</p> <p>Application Access supports regular expression for flexibility in authorization and for better security</p> <p>Support hierarchical roles-based groups i.e.</p> <ul style="list-style-type: none"> • Students groups has undergraduates groups and graduates groups • Undergraduates groups has first year students, etc 	<p>Able to create a group that is cross application with hierarchical rules-based groups support i.e.</p> <ul style="list-style-type: none"> • Group a student from rural areas • In Financial System, give the group a special tuition rate • In E-Learning, monitor the group contributions • In Student Information System, monitor the grade's of each member in the group
Output	Single Sign –On	System Management Consolidation	Cross-Application Services

6 Cross-Application Audit

Audit and tracking can be done on user activities that can profile user activities across all applications within certain time. Some of the cross applications audits are

- Authentication reports & statistics with multi-dimensional scope (success/failed rates across all apps)
- Authorization statistics (success/failed rates across all apps)
- History & Scheduled Reports (Daily/Monthly/Quarterly)
 - Group history (all changes to all group profiles)
 - Identity history (by user)
 - Users created/deactivated/reactivated/deleted
 - User profile modification history (for all users)
- Failed authorizations (by user)
- Password changes (in a particular interval of time)
- Deactivated users report
- Audit of user activity

8 Cross-Application User Provisioning

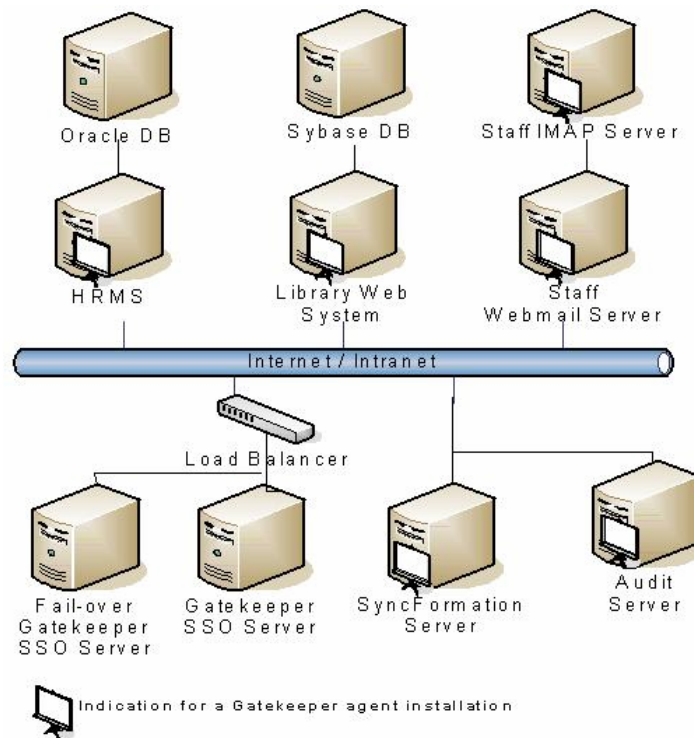
	User Experience	System Administrator Experience
Features	<p>New User such as new student will be given a single username that have accesses to all permitted applications during registration day.</p> <p>The student will be given a temporary password that may last about an hour. With that temporary password, the student will have to change his password according to his liking.</p> <p>If a user is terminated, the user will not be able to access all application immediately.</p>	<p>Administrator will use less time to manage users and groups for each application. Now, many user and group management are just in a click of button. The new ways of provisioning between applications are</p> <ul style="list-style-type: none"> New Normal User/Group Provisioning Users/Groups Archiving Changing Users Information User Suspension Special User Creation Temporary User Creation <p>Administrator does have to manage creating new user in SIS, Student Portal, Library System, Email, E-Learning System etc.</p>
Output	Reduce Unproductive Time	System Management Consolidation

9 Strategic Benefits

Return on Investment (ROI) on Existing Heterogeneous Applications	Reaping more profitability through cross-application functionalities with more productivity, more efficiency, more effectiveness and more competitiveness.
Consolidation of System Management	Consolidate profiles, identity, accesses, policies, provisioning Better Organizational Control
Consolidation of organizational knowledge	Real-time Human Resource Capability & Capacity for Allocation Consolidate audit for consolidation of transactions and user activities (e.g. analyze a person from activities in HR System, Staff Portal & e-learning portal, and FIS)
Cross-Application Services	Organization can create a service that aggregates services from each application such as e-learning, student portal and student info system.
Containment of operational risk	Each user activities and access can be managed centrally Better Network Security
More Productive Resource (Human, Money, Time)	Increase Productivity of all stakeholders in applications environment System Owners, System Developers, End Users, System

	Administrators, Helpdesk Low Switching Cost: Easy Deployment into Existing Applications
Strength	Proven track record: 35,000 users

10 Sample System Architecture



11 Contact Information

For more information, please contact us at

Nervesis Sdn Bhd

Catalyst ECC Center, Incubator 3, Level 4, Universiti Kuala Lumpur,

Bandar Wawasan 1016, Jalan Sultan Ismail, 50300 Kuala Lumpur

Phone: +603 4147 5266 Fax: +603 4108 5266

Contact Person: Azhar K Mustapha

Email: azhar@nervesis.com.my