# DESIGN AND IMPLEMENTATION OF A SINGLE SIGN-ON SOLUTION

A thesis written at

**MIKA SYSTEMS, INC.**

and submitted to

**KETTERING UNIVERSITY**

in partial fulfillment
of the requirements for the
degree of

**BACHELOR OF SCIENCE IN COMPUTER SCIENCE**

by

**KEVIN L. HELPINGSTINE**

September 29, 2007

_____
Author

_____
Employer Advisor

_____
Faculty Advisor

## DISCLAIMER

This thesis is submitted as partial and final fulfillment of the cooperative work experience requirements of Kettering University needed to obtain a Bachelor of Science in Computer Science Degree.

The conclusions and opinions expressed in this thesis are those of the writer and do not necessarily represent the position of Kettering University or my employer, or any of its directors, officers, agents, or employees with respect to the matters discussed.

## PREFACE

This thesis represents the capstone of my five years combined academic work at Kettering University and job experience at Mika Systems, Inc. Academic experience in Computer Science proved to be a valuable asset while I developed this thesis and addressed the problem it concerns. Although this thesis represents a compilation of my own efforts, I would like to acknowledge and extend my sincere gratitude to the following persons for their valuable time and assistance, without whom the completion of this thesis would not have been possible:

1. My parents, for supporting me throughout my college career and beyond.
2. Dr. Jim Huggins, Associate Professor of Computer Science at Kettering University, for offering trustworthy advice and answering hard questions directly.

## TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

**Figures** **Page**

# I. INTRODUCTION

## Problem Topic

As Sallie Mae Home Loans grows as a company, their computer networks must also expand to meet the needs of their employees and customers. Their recent rapid growth has led to requiring several different user names and passwords from each user. This increase in complexity has caused a general decrease in productivity among the IT staff and the loan officers to which they provide service.

## Background

In the past year, Sallie Mae Home Loans (SMHL) acquired offices in both Arizona and Massachusetts, greatly expanding the number of loan officers who needed access to their applications. This increased the amount of services that the IT group needed to provide, as well as the overall technical support load. Unfortunately, not all computer systems are designed to easily inter-operate. Integrating the authentication of these disparate applications within one central database presented a great challenge for SMHL's IT staff, so they requested that Mika Systems design a single sign-on solution for their network.

## Criteria and Parameter Restrictions

In order for the project to be considered a technical success, users must be able to login to their workstation with a SecurID keyfob and automatically have access to multiple computer systems and applications. Specifically, users must be able to access the corporate

Contact Resource Management (CRM) application, Microsoft Windows data shares, and Open-Xchange Groupware. Secondly, the administration of the system must be centralized and easy to maintain. Finally, a preferred solution would only duplicate a user's data in a minimum number of locations, or in one central Oracle database.

## Methodology

The process used in the development of this software borrows heavily from the Waterfall Model of software engineering. The steps of this model are:

1. Requirements
2. Specification
3. Planning
4. Design
5. Implementation
6. Integration
7. Maintenance

The preceding seven steps are divided into four stages. The first stage, "Analysis," encompasses the gathering of requirements and creation of a simple specification by the software engineer. A number of possible solutions will be considered in this stage and the software engineer will discuss the options with the customer to determine the best option to pursue. The second stage, "Design," contains the next two steps, planning and design, in the Waterfall Model. In the design stage, the software engineer takes the specification created in the analysis stage and creates a methodology to solve the problem. Next, the third stage, "Implementation," contains the implementation and integration. One very important part of this stage is continuous testing of code and software. Finally, the code is placed into the

last stage, maintenance. Maintenance is generally for predicting and solving any problems that might occur during the life of the solution, such as hardware upgrades, related software upgrades, or regulatory changes.

The Waterfall Model and the four stages are not monolithic and will almost always be deviated from in some way. A developer may have to revisit the design and planning stages at any time during the development cycle. For example, problems might arise in the implementation stage that cannot be solved in a cost efficient way and a revision to the design may be necessary. The entire process also tends to restart when new features are requested.

## Primary Purpose

This thesis presents the results of investigating potential single sign-on solutions.

## Overview

Chapter II contains an analysis of the requirements devised by MIKA Systems, Sallie Mae Home Loans, and the author. Next, Chapter III contains design and related information for the project. Chapter IV discusses the implementation, testing, and integration of the final solution. Finally, Chapter V contains conclusions, recommendations, and possible future developments.

# II. REQUIREMENTS AND ANALYSIS

## Overview

This section begins with the primary requirements of the solution. The problems encountered in the requirements phase are also discussed.

## Features

Sallie Mae Home Loans (SMHL's) most important request for the single sign-on was for the system to be easily maintainable. This means, primarily, that there should be a minimum number of steps required for management of both users and computers. Currently, their entire user database is stored in Microsoft Active Directory (AD) and authentication is handled by RSA Ace Server (ACE). Users are created in AD and regularly synchronized with ACE. Unfortunately, this only allows for users to log into the Microsoft Windows network and not to applications such as their CRM or email.

A key feature required of SMHL's single sign-on solution is ease of maintenance of access lists (*SMHL Meeting Notes*, 2005). This is the most important feature to the customer. Currently, they maintain no fewer than four user databases on different servers running different operating systems. The single sign-on will replace these four separate databases with only the Windows AD ideally. Microsoft provides great GUI tools for administration of user accounts and permissions, so it will be used for the primary user database. The Microsoft AD user management tool can be seen in Figure 1.

Using ACE will also allow SMHL IT to use ACE's built-in user administration tool,

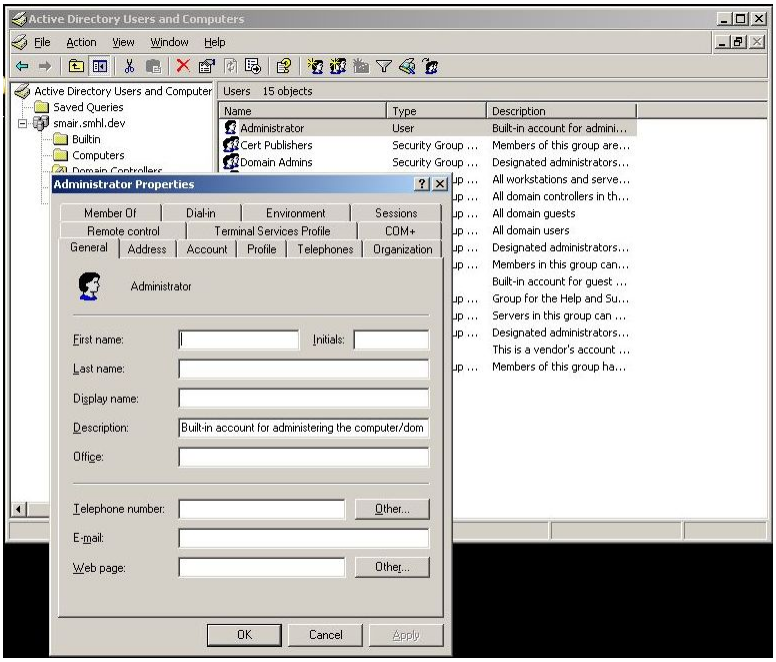


Figure 1 Microsoft Active Directory user management tool.

which can be seen in Figure 2. This tool may be used in the event a special user is to be created that may be unwanted in the Windows environment. An example of such a user would be a remote administration account specific to a single UNIX system. The RSA user tool synchronizes with AD on a regular basis as determined by SMHL. This provides the system administrators with flexibility for the administration of users.

Another major feature required of the single sign-on was to appear simple and unobtrusive to users. This was achieved through integration with their Windows desktops and terminal servers. Every desktop and terminal server has had the login interface replaced with software to facilitate the secure use of the single sign-on system, but the change is visibly unobtrusive from a user's perspective. Figure 3 illustrates a comparison of the two login interfaces.

Finally, all efforts were made to either be forward-compatible or at least standards compliant with regard to off-the-shelf software packages like the ACE Server. In the case of a major upgrade in the core software that SMHL employs, the impact to the single sign-on

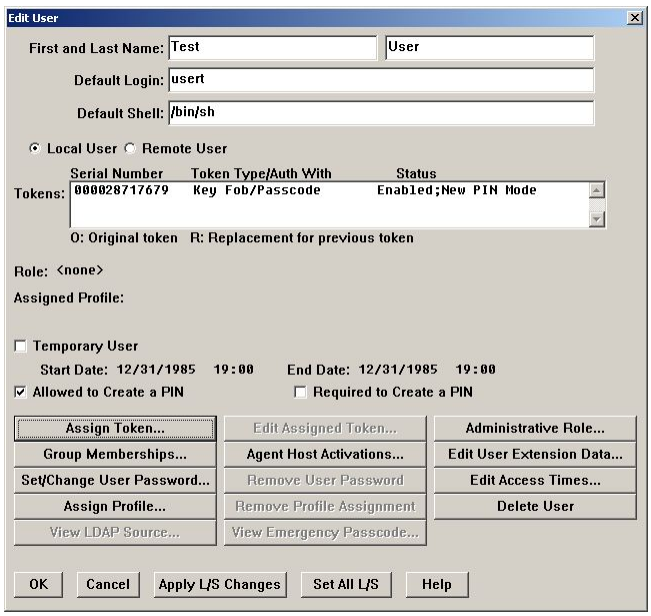


Figure 2 RSA Ace Server user management tool.

should be minimized wherever possible.

## Problems Encountered

The goals of the project were stated very simply and clearly. Through regular meetings, the team was able to simply avoid most problems due to the great working relationship with the SMHL IT group. Their technical knowledge made them an asset that allowed us to quickly determine the basic requirements of the project. Overall, the design phase of the project was free from technical problems, but there was a major threat of ”feature creep”. Shortly after beginning the project, the decision was made to bundle in a replacement for a large module in the CRM application. Unfortunately, this was included in the overall deliverables of the project but is beyond the scope of this document.


Figure 3 Standard Windows login and the replacement Windows login.

# III. DESIGN AND SPECIFICATION

## Overview

This chapter describes the design stage of the single sign-on system. A detailed description of the architecture of Sallie Mae's network is discussed first, followed by an explanation of the single sign-on login processes, and finally a brief note on options for implementing the application login.

## Current Architecture

Sallie Mae Home Loans' (SMHL's) existing computer network is laid out as described in Figure 4. They have a single Windows 2003 AD Domain supported by an RSA ACE server. The AD server provides authentication to the user and administrator terminal servers based on information on the ACE server. Once a user has logged into their assigned terminal server, they may still require many different sets of login information to access the Internet, the company CRM application, and other resources on the company intranet. The login information is stored on many different servers, including, but not limited to relational databases and AD. Currently each application maintains its own authentication database creating a difficult to manage environment.

## Windows Login Process

To the user, the login to network resources should be transparent. They simply log into their workstation or assigned terminal server and from there they should be provided

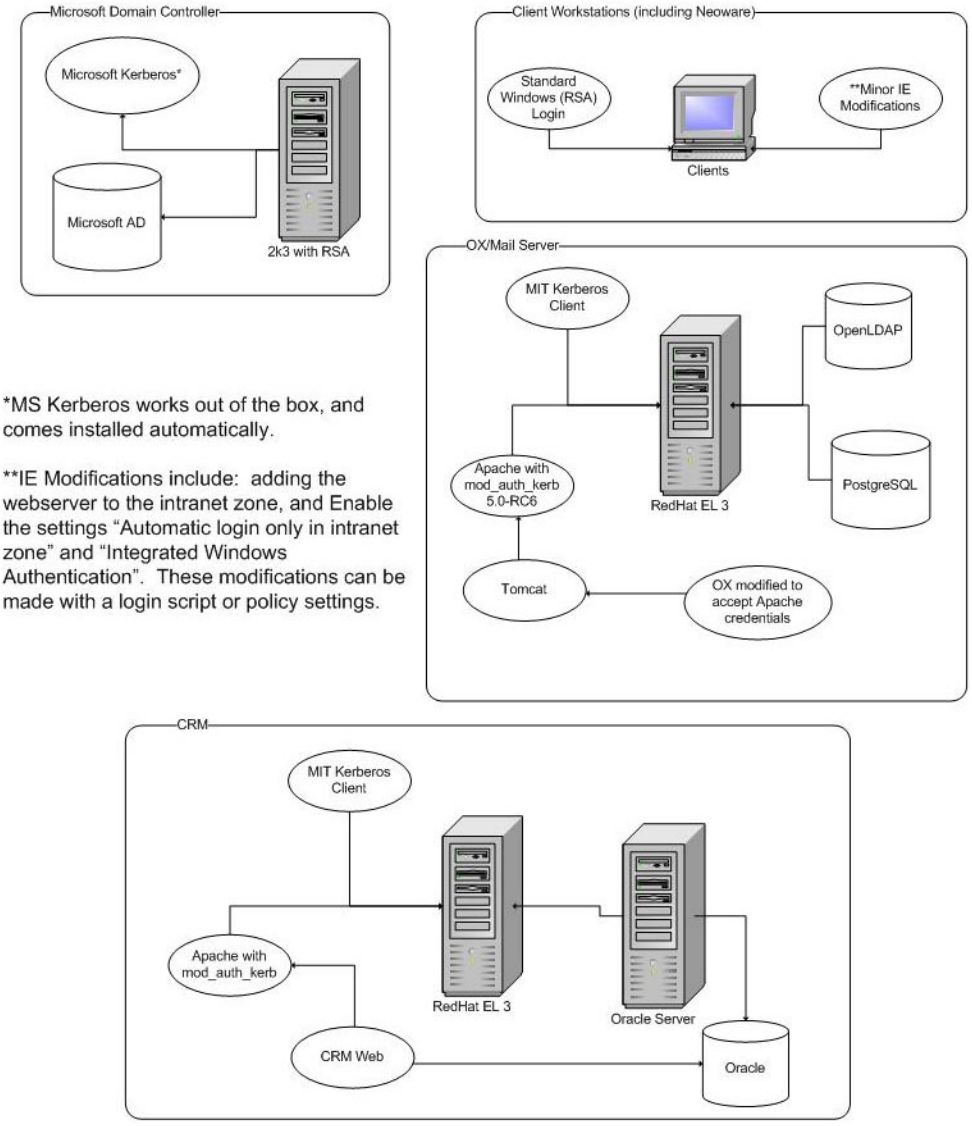


Figure 4 SMHL Network.

access to any network resource they require without having to reauthenticate. The login component of workstations and terminal servers were replaced by the RSA SecurID login component for all users. This allows the use of the SecurID keyfobs for authentication of the user. The login information is passed to the RSA ACE Server by Windows where it is verified. Next, the SecurID server will authorize the Windows domain controller to issue a Kerberos ticket to complete the login process. The Kerberos ticket issued by the Active Directory Server is maintained by the user's workstation or terminal server session and is sent to whatever application requests it.

**Application Login Process**

SMHL's primary application is their CRM which is used to track leads and loans in progress. It is a web application written in PHP with an Oracle database backend. In order to support the single sign-on the authentication code must be rewritten to support Kerberos natively or through the application web server. It was decided that the web server would be the simplest place to support the Kerberos authentication and would have the least development time and impact on the stability of the CRM.

When a user successfully logs in to a website that requires authentication Apache set the REMOTE_USER environment variable to the user name used to authenticate. This variable is already used in the CRM to check a user's authorization level but in order to reduce necessary code changes the code was be modified to trust the existence of the environment variable as proof of valid authentication. This method is to be used for all other web applications including the SMHL intranet.

**Application Login Implementation Options**

Before settling on mod_auth_kerb for Apache an older method was briefly discussed involving NTLM authentication. It was determined that this outdated technology should not be maintained due to security concerns. The main concern being the possibilty that

Microsoft might drop support for NTLM in later versions of Internet Explorer. Kerberos, on the other hand, is an open standard and would even allow the use of alternative browsers such as Mozilla Firefox or Opera.

# IV. IMPLEMENTATION, INTEGRATION, AND TESTING

## Overview

This chapter begins with the process used to design a development environment for the single sign-on system, then describes the tools used. Integration of the system with Sallie Mae's network infrastructure is covered, and the testing process of the system is described. Problems encountered with the tools and the development environment are noted throughout.

## Building a Development Environment

In order to properly build and test the single sign-on solution for SMHL, we first needed to create a replica of their production environment. Due to budget constraints, we were given only two machines with which to attempt to closely match a network consisting of many more. One machine (OX) was dedicated to hosting UNIX services such as the CRM and Open-Xchange while the other (SMAir) was dedicated to hosting Windows services like AD and the RSA ACE server. Clients were simulated using virtual machines on the author's desktop computer using VMWare.

To minimize potential problems when migrating a finished product, we compiled an inventory of software currently in production and based all of our development off of that. While upgradability was definitely a concern, starting from a stable base line was important when faced with a piece of software that we were unable to control. Red Hat Linux Enterprise Server was installed on OX with custom builds of PHP, Perl, and Apache to

maintain compatibility with the existing applications. SMAir runs Windows Server 2003 with a patch set comparable to SMHL's production terminal servers and RSA ACE Server 6.0. The client machines were running Windows XP Professional and Windows 2000 Professional under VMWare.

### Tools

Primary development of the CRM and Open-Xchange was done on Linux servers. The MIT Kerberos V tools and utilities were used for accessing the Windows AD from these servers. Subversion, an open-source version control system, was used for source code version tracking and remote access to code throughout the project. On SMAir, the Microsoft Windows 2003 Support Kit was used to generate host and service keys.

Difficulties arose with generating the shared keys so that the Linux servers could authenticate with the AD. Poor documentation led to the need to use trial and error to find the proper commands to generate the keys. The resulting commands are listed in Appendix B.

### Integration

Integration into SMHL's current network infrastructure was studied but never implemented due to cancellation of the beta phase of the project. Nonetheless a plan exists for integrating the single sign-on into the production SMHL network.

Kerberos requires that every computer participating have its clock synchronized within five minutes of the key server's clock. This is required because the request for authorization is based on the current time on the requesting machine. The AD server synchronizes its clock with public network time servers over the internet and all of SMHL's internal computers sync with it. Unix machines run xntpd to maintain the synchronization and Windows clients have a built-in service.

The service and host users and keys are generated and distributed to their target machines. The CRM, OX, and intranet web servers will be configured with two authentication

methods: the Kerberos method and the standard existing authentication methods. Once the system is matured and stable the previous authentication methods will be removed at the discretion of the SMHL IT department.

Clients must also be updated in order to support automatic logins to the web servers. Login scripts are generated to add the target hosts into the Internet Explorer ”Trusted Sites” and to enable the ”Integrated Windows Authentication” option.

## Testing

Extensive testing of the login system was conducted in the author's development environment. Primarily, testing focus was on determining whether or not the system would function as expected when a user moved from a terminal server to a physical computer and back. Different combinations of user privileges were tested to determine if, for example, disabling remote access would affect the user's ability to authenticate from a terminal server or from their workstation.

An excessive load was placed on the CRM web server using a log of past traffic to verify that, even under heavy loads, the authentication requests would still succeed. While the database and the web server were severely taxed, the AD server was able to continue issuing authentication tickets without difficulty. From this it was determined that the application and database would provide a scalability problem long before authentication would become a bottleneck.

# V. CONCLUSIONS AND RECOMMENDATIONS

## Conclusions

The system met all of the criteria set forth in Chapter 1. Every test user assigned a SecurID keyfob was able to access multiple servers and applications having logged in only once on their local workstation or terminal server. The intranet and CRM applications are integrated into the system along with Open-Xchange. User administration was performed through the central Microsoft and RSA utilities which already were in use, reducing necessary system administration time. Unfortunately, due to more control of the SMHL IT department being taken over by Sallie Mae Corporate the single sign-on project was placed on an indefinite hold before onsite beta testing could begin.

## Recommendations and Future Developments

Due to the lack of onsite beta testing the number of recommendations for future development are limited to observations of the author during development and alpha testing. If beta testing is ever allowed, some of these suggestions may be considered.

If SMHL continues to grow at its current rate, the CRM and this single sign-on will need to be reevaluated for scalability. A credential caching system could potentially reduce the number of authentication requests to the AD server by a great deal and is in use by competing commercial offerings. In the current environment there should be no problem with a single server handling all of their authentication requests, but if the amount of data queried or the number of requests grow substantially the system could become quite slow.

In the interest of keeping the system as simple as possible for initial testing, more advanced features of the Kerberos V authentication protocol were not utilized (*SMHL Meeting Notes*, 2005). Some of these features, like ticket delegation, would allow for finer grained access control in SMHL's custom applications. This would be a very desirable feature and potentially could improve the security and flexibility of all of the target networked applications.

Another potential expansion of the project in which the management at SMHL expressed interest was biometrics, specifically, replacing or supplementing the SecurID key fob with a device like a fingerprint scanner in order to further reduce the impact on users, and increase security (Webber, 2005).

After the completion of the project a commercial product by Centrify corporation was discovered. Centrify's DirectControl suite would serve the same purpose as this in-house single sign-on without the cost of maintaining the in-house project. DirectControl supports several more advanced features, such as credential caching and even database single sign-on.

## REFERENCES

*SMHL Meeting Notes.* (2005).
Webber, D. (2005, July). *Personal interview.*

# APPENDICES

# APPENDIX A

# OPEN-XCHANGE PATCH

Due to space limitations the Open-Xchange patch is not included. It can be retrieved online from http://www.reprehensible.net/~ sig11/OX/

```
create tablespace ox
  logging
  datafile '/oracle/oradata/ox/ox.dbf'
  size 32m
  autoextend on
  next 32m maxsize 2048m
  extent management local;


CREATE USER ox
       IDENTIFIED BY ox
       DEFAULT TABLESPACE ox
       TEMPORARY TABLESPACE temp;


GRANT CREATE SESSION TO ox;
GRANT CREATE TABLE TO ox;
GRANT CREATE VIEW TO ox;
GRANT CREATE SEQUENCE TO ox;

ALTER USER ox QUOTA unlimited ON ox;

GRANT CREATE SESSION TO pcc;
GRANT CREATE TABLE TO pcc;
GRANT CREATE VIEW TO pcc;
GRANT CREATE SEQUENCE TO pcc;
```

# APPENDIX B

# CONFIGURATION FILES

```
To create a Windows Kerberos keytab:
First create a user in Active directory to represent the service...
ktpass -princ HTTP/CRM.ox.smhl.com@ox.smhl.com -mapuser CRM -pass PASSW
Copy crm.keytab to ox.smhl.com:/etc/

Added to the Apache httpd.conf:
LoadModule auth_kerb_module libexec/mod_auth_kerb.so
<Directory />
AuthType Kerberos
AuthName "SMHL Intranet"
KrbMethodNegotiate On     #Enable GSSAPI auto-login
KrbAuthRealms SMAIR.SMHL.COM
Krb5KeyTab /etc/crm.keytab #Each directory can have its own service key
require valid-user
</Directory>


krb5.conf:
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 ticket_lifetime = 24000
 default_realm = SMAIR.SMHL.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false

[realms]
 SMAIR.SMHL.COM = {
  kdc = smair.smhl.com:88
  admin_server = smair.smhl.com:749
  default_domain = smhl.com
 }

[domain_realm]
 .smair.smhl.com = SMHL.COM
 smair.smhl.com = SMHL.COM

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
```

```
  forwardable = true
  krb4_convert = false
}
```

# APPENDIX C

# PROGRAM OUTCOMES

The design and implementation of the single sign-on solution has demonstrated the author's ability to take the problem solving skills and theoretical background taught by the computer science department at Kettering University and apply them to entirely different real-world problems. The important concepts and skills provided a solid foundation for continued learning.

During the development of the single sign-on solution the author used his skills, professionalism, confidence, and experiences to communicate effectively with customers and co-workers to develop a working solution.

The development of the single sign-on solution required close communication with the customer and with other members of the development team. Communication skills learned at Kettering University were vital to the success of the project.

The hands-on lab experience provided by the computer science faculty at Kettering University was important at every step of the project. Problem solving skills learned in the laboratories and in the classroom were utilized every day by the author.