

# Sunshine Connections

## Account Maintenance

### Physical Design

Author Bob Pfeiff  
Author Position Architect  
Date 9/29/2005

Version: 1.0

Final

© 2002 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. **MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.**

Microsoft and Visual Basic are either registered trademarks or trademarks of Microsoft in the United States and/or other countries.

## Table of Contents

Sunshine Connections.....	1
Account Maintenance .....	1
Physical Design .....	1
Revision & Sign-off Sheet.....	<b>Error! Bookmark not defined.</b>
Table of Contents.....	1
Physical Design Summary.....	2
Environment Constraints, and Assumptions .....	2
Dependencies.....	3
The password management application depends on the following software environment: .....	3
1. Windows 2003 Server configured as a web and application server .....	3
2. Windows 2003 Active Directory (using ADSI) .....	3
3. SQL Server 2000 .....	3
4. SSL certificate for the Sunshine Connections web site .....	3
It also depends on server hardware hosted at the DOE data center to support the software listed above. ....	3
Project Dependencies .....	3
Application Development.....	3
User Services (UI – User Interface) .....	3
Component ASP.Net Application Design .....	6
Business Services (Middle-tier Business Logic).....	7

## Physical Design Summary

The password management application for Sunshine Connections will provide end users with the ability to change their Active Directory passwords and to recover forgotten passwords. This functionality is necessary to relieve DOE and school district administrators of having to manage passwords for the more than 200,000 planned users of Sunshine Connections.

The password management application will be implemented using ASP.Net to make ADSI calls to make password changes in the Sunshine Connections Active Directory, and to store “secret questions” and a hash of the users’ answers to those questions in a SQL Server database. This application will support three scenarios:

1. The user knows their existing password and wants to change it.
2. The user knows their existing password and selects three “secret questions” from a list and provides answers to those questions to verify their identity if they need to reset a forgotten password.
3. The user has forgotten their password and needs to reset it.

## Environment Constraints, and Assumptions

Since Sunshine Connections has its own Active Directory for the purposes of authenticating users and a network and server infrastructure to support both web application and database components, the password management application can be hosted with Sunshine Connections. Secure Sockets Layer (SSL) encryption of internet traffic between users and Sunshine Connections has also already been implemented so the password management application can take advantage of SSL for protecting the sensitive data it manages.

The decision to build a custom password management system for Sunshine Connections versus using an off-the-shelf product was two-fold. First, since this is a business investment project for Microsoft, the cost of licensing an off-the-shelf product were a concern; second, the scope of the required functionality is narrow enough that development of a password management application was relatively inexpensive using the tools readily available to the project team.

While the Sunshine Connections architecture includes an XML Web Services layer that will be used in implementing most functionality, use of this layer for the password management application was not deemed necessary because the application is strictly end-user facing and its business logic is very simple making the use of intermediate web services components inefficient from both a development and application performance point of view.

The following assumptions were made:

1. DOE, school district, and other participating organizations can not support password management for Sunshine Connections users (200,000+ projected)
2. Password policy for Sunshine Connections is set by the DOE and will vary from school district and other participating organization policies
3. The “secret questions” must comply with the most stringent password management tool in use among the four pilot school districts so they are based on the password management rules at Miami Dade County Public Schools

## **Dependencies**

The password management application depends on the following software environment:

1. Windows 2003 Server configured as a web and application server
2. Windows 2003 Active Directory (using ADSI)
3. SQL Server 2000
4. SSL certificate for the Sunshine Connections web site

It also depends on server hardware hosted at the DOE data center to support the software listed above.

### ***Project Dependencies***

This development effort requires a web developer with deep experience in ASP.Net and knowledge of ADSI, SQL Server data access, and user interface design. It also requires the server environment described in the dependencies section above to be in place and approved for use by external users by the combined DOE/Microsoft partnership team.

## **Application Development**

The password management application will consist of components developed in ASP.Net and SQL Server. The application will query and manipulate user account information in the existing Active Directory using ADSI, and store “secret question” and answers to those questions for each user in a SQL Server database.

Answers to “secret questions” will be stored in the database using a one-way hash. If a user needs to input their answers to reset a forgotten password, the hashing algorithm will be applied to the answers they supply and compared to the hash value in the database.

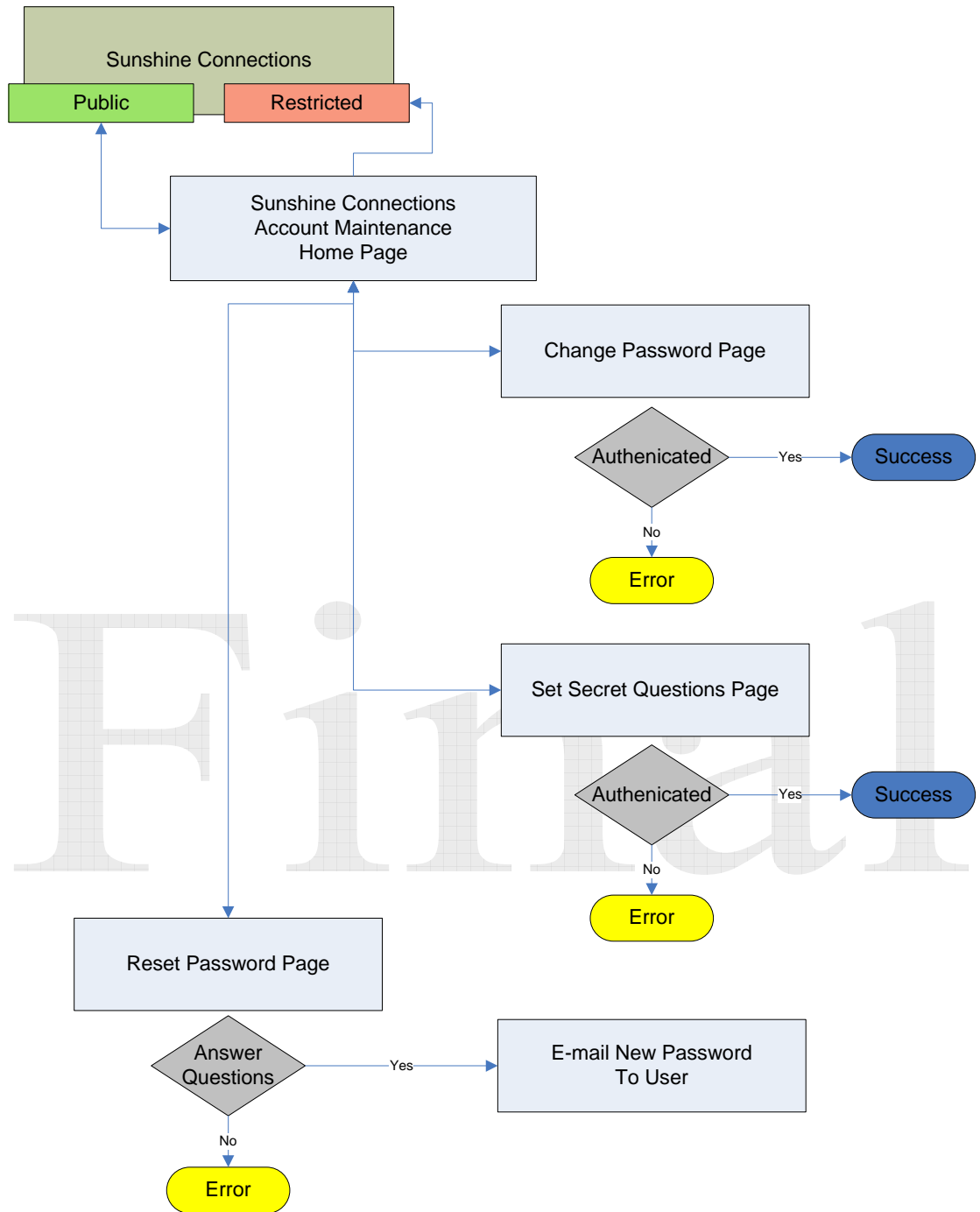
### ***User Services (UI – User Interface)***

The UI for the password management application will consist of:

1. A home or start page with links to Change Password, Set Secret Questions, and Reset Password, the home page will also have links to the Sunshine Connections public and restricted areas.
2. A Change Password page where a user who knows their password can change it.
3. A Set Secret Questions page which will allow an authenticated user to select three secret questions and provide answers to them to validate that user in case they forget their password.
4. A Rest Password page that allows a user to reset a forgotten password after correctly answering their three secret questions.

Users must have a valid user account login name, and password to be authenticated. If the user has forgotten their password, they must provide a valid user account login name and correctly answer three “secret questions” for the application to e-mail them a new system-generated password. The following diagram shows a site map and flow for the password management application.

# Final



*Password Management Application Site Map/Flow*

## **Component ASP.Net Application Design**

The primary user interface components will be implemented as a web application using ASP.Net. The user interface components will not be implemented within the Windows Sharepoint Services site that hosts other Sunshine Connections functionality to simplify the security implementation for the password management application, and to make it a more portable solution. The user interface is designed to present a simple set of functions for end-users to manage their passwords without additional assistance from their local school district help desk or Sunshine Connections administrators. The screens for this user interface are depicted below.

### ***Behavioral Summary***

The ASP.Net application component provides three actions for users to perform:

1. Change their password
2. Set their secret questions and answers for password recovery
3. Reset their password using their secret questions and answers

The user will receive a message at the bottom of each screen indicating the success of the action they attempted. In the case of the submission of an incorrect user name and/or password, or if an error occurs, the user will be directed to contact a system administrator.

### ***Dependencies***

The ASP.Net application component depends on:

- Windows Server 2003 configured as a web and application server with an SSL certificate installed for secure communications via https
- SQL Server database that contains both a list of secret questions, and the list of selected secret questions and their answers, whose values are hashed, for each user
- Active Directory (via ADSI), which is used to authenticate the users' input credentials and may be modified by the application depending on the user action

### ***Error Messages***

Errors handled by the ASP.Net component are:

- Incorrect user name and/or password
- Incorrect answer(s) to secret questions
- No e-mail address on file (for e-mailing new system-generated password after password reset)
-

### ***Security Implementation***

The ASP.Net component requires the input of a valid Active Directory user id and password to change a password and to select secret questions and input answers to those questions.

Access is controlled by user, not role, since the functions of the application affect individual user accounts.

### ***Component Management Issues***

The ASP.Net component runs in IIS on Windows 2003 Server.

### ***Business Services (Middle-tier Business Logic)***

The business services of the password management application are:

# Final