



Sunshine Connections

Identity Management

Active Directory Federation Services (ADFS)

Final

© 2008 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.

Overview

In developing the identity and access management strategy for Sunshine Connections, the FL-DOE understood that requiring individual school districts to maintain duplicate user credentials is not always desired. Leveraging the existing Active Directory infrastructure in each school district for user authentication alleviates users from having to remember another userid and password.

In Microsoft Windows Server 2003 R2, a new technology component – Active Directory Federation Services (ADFS) – was introduced to facilitate web single sign-on. This is accomplished using the WS-* interoperability protocols, specifically the WS-Federation protocol. ADFS provides an extensible architecture that supports the Security Assertion Markup Language (SAML) token type and Kerberos authentication (in the Federated Web SSO with Forest Trust scenario).

General Architecture

ADFS consists of two key server components, the Federation Server and Federation Server Proxy. The Federation Server is responsible for defining the trust policies and claims between organizations. The Federation Server Proxy is strictly used to facilitate clients from an account forest to authenticate when they are connected to the Internet and not the corporate network.

Server Roles

Federation Server

- STS (security token service)
- Issues security tokens
- Populates claims
- Statements an authority makes about security principals
- Manages federation trust policy

Federation Server Proxy

- Client proxy for token requests
- Provides UI for browser clients

ADFS Web Agent

- Enforces User Authentication
- Creates User Authorization Context

Web Application

- NT Impersonation and ACLs
- ASP.NET IsInRole()
- AzMan RBAC integration
- ASP.NET Raw Claims

Active Directory

- Authenticates Users
- Manages Attributes