



Securing Cloud Applications Using Windows Azure Access Control



January 20, 2012
Keith Franklin
Director of Cloud and .NET Services

www.mpspartners.com

MPS Partners Overview

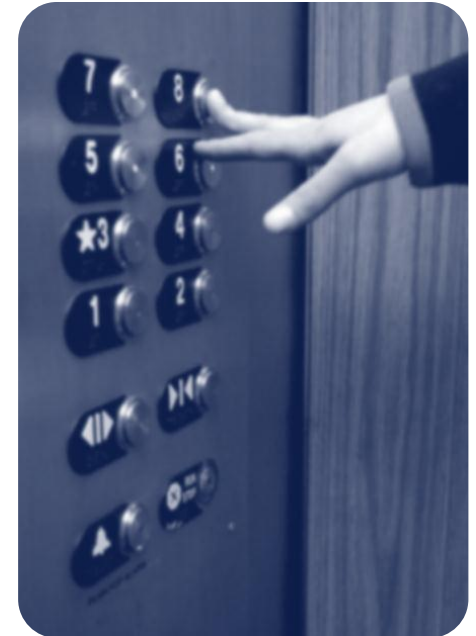
Claims based Identity. What is it?

Windows Identity Framework (WIF)

WIF and Windows Azure

Securing a Web Applications using Windows
Azure Access Control Service

- MPS Partners is a Microsoft Gold Certified Managed Partner with deep expertise in defining and deploying solutions based on Microsoft technology
- We focus in a few key areas:
 - ◆ Collaboration and enterprise content management
 - ◆ Business Intelligence
 - ◆ Integration of the Microsoft toolset with diverse technology landscapes and the cloud
 - ◆ We are especially known for having this expertise within accounts that run SAP



- Founded in 2006, MPS Partners is **Microsoft's 2010 Central Region Partner of the Year**. We have earned the distinction of being a Microsoft Gold Managed Partner – an elite designation within the Microsoft partner community.
- Our experienced staff and leadership team are business people first that focus on bringing valuable **business solutions** to market.
- We are part of **SPR Family of Companies**, a 35-year-old professional services firm headquartered in the Willis Tower in Chicago, IL.



SOA and Business Process
Information Worker Solutions
Business Intelligence
Custom Development Solutions

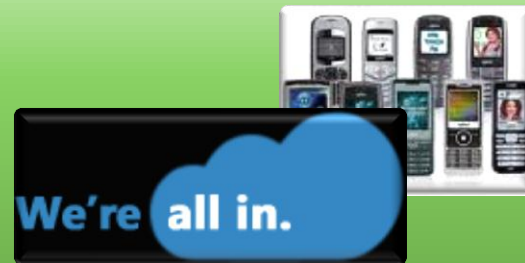


Application Platform and Integration



- BizTalk Integration Solutions
- Enterprise Service Bus
- Cloud Integration
- Supply Chain Solutions

.NET and Cloud Solutions



- Advanced .NET Solutions
- Windows Azure Development
- Mobile Solutions

Providing Technology solutions that magnify the value of previous IT investments and enhance communication with business partners.

MPS Partners Overview

Claims based Identity. What is it?

Windows Identity Framework (WIF)

WIF and Windows Azure

Securing a Web Applications using Windows
Azure Access Control Service

- Identity
 - ▶ For sake of this discussion think of Identities as “Users”
- Tokens
 - ▶ A bunch of bytes that represents an Identity
 - ▶ Usually XML in the form of Security Assertion Markup Language (SAML)
- Claims
 - ▶ Represent something about the Identity (Name, Age, Position, etc.)
 - I claim that I am Keith Franklin
 - I claim that I am 45
 - ▶ Contained within a Token
- STS – Security Token Service
 - ▶ Software that issues Tokens

- Identity Provider
 - ▶ Combination of a STS and an Account/Attribute Store
 - ▶ Examples:
 - Active Directory Federation Services 2.0
 - Windows Live ID, Facebook, Yahoo, Google
- Federation Provider
 - ▶ Service that takes multiple trusted or untrusted Identity Providers and produce a trusted Identity Token to an application
 - ▶ Examples:
 - Windows Azure AppFabric Access Control - Cloud
 - Active Directory Federations Services 2.0 – On Premise
- Identity Library
 - ▶ Windows Identity Foundation

MPS Partners Overview

Claims based Identity. What is it?

Windows Identity Framework (WIF)

WIF and Windows Azure

Securing a Web Applications using Windows
Azure Access Control Service

- Programming Model
- Software Development Kit (SDK)
 - ▶ Provides pre-built .NET security logic
 - ▶ Visual Studio Tools/Wizards
- Middleware Technology for building Claims aware solutions
- Allows for Applications to be built that are unaware of how they are secured.
- When un-authenticated visitor arrives the Middleware steps in and authenticates the user and upon success the user and the users security token is redirected to the intended application.

MPS Partners Overview

Claims based Identity. What is it?

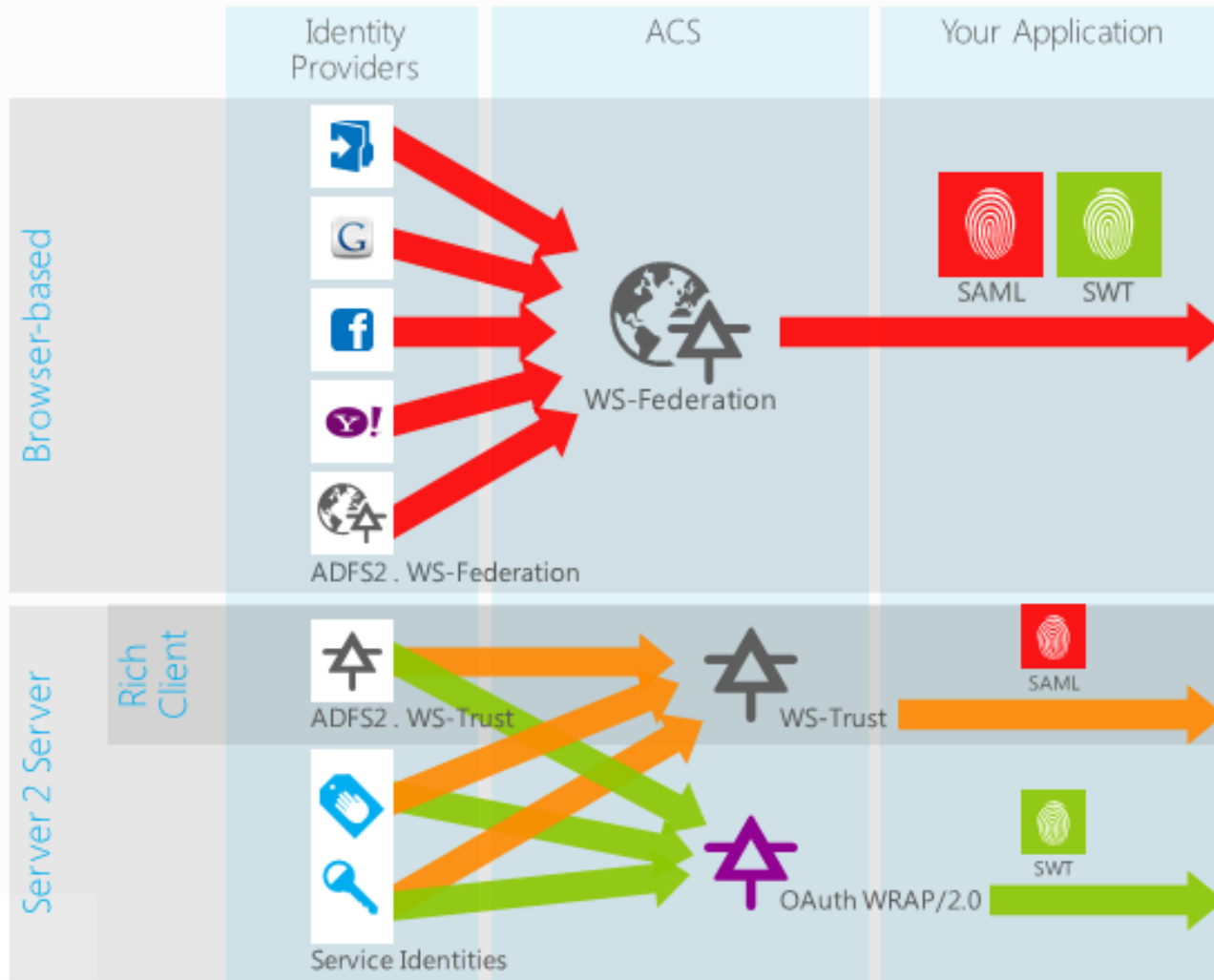
Windows Identity Framework (WIF)

WIF and Windows Azure

Securing a Web Applications using Windows
Azure Access Control Service

- Windows Azure Access Control Service (ACS)
 - ▶ Supports Web Application single sign-on (SSO)
 - ▶ WS-Federation
 - ▶ Federation for SOAP and REST Web Services using WS-Trust and Oauth
 - ▶ Web Based Management Portal
 - ▶ Odata-based management service for configuring and managing the service
- WIF provides the plumbing for your applications to integrated with ACS

ACS





1. User enters page address in a browser
2. Page responds to browser to redirect to ACS
3. Browser asks ACS for a Token
4. ACS responds with list of Token types to user
5. User logs in to Identity Provider
6. Identity Provider returns Token to browser
7. Browser presents Identity Provider Token to ACS
8. ACS returns an ACS Token to browser
9. Browser redirects back to original page address with ACS Token
10. Page responds accordingly

MPS Partners Overview

Claims based Identity. What is it?

Windows Identity Framework (WIF)

WIF and Windows Azure

Securing a Web Applications using
Windows Azure Access Control Service

- Demo
 - ▶ Use WIF and Windows Azure Access Control to secure a Web Role (ASP.NET Web Site)

- Additional Information
 - ▶ Azure SDK
<http://www.microsoft.com/windowsazure/sdk/>
 - ▶ Azure Platform Training Kit
<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8396>
Microsoft Windows Azure Development Cookbook by Neil Mackenzie
 - ▶ Windows Identity Foundation Simplifies User Access for Developers
<http://msdn.microsoft.com/en-us/security/aa570351>
- Need assistance with Azure contact MPS Partners, LLC
 - ▶ Keith.Franklin@MPSPartners.Com