



# Claims Authentication and SharePoint 2010

---

Tyler Durham, Technology Solution Professional  
Microsoft Corporation

# About Me

- For six years, I travelled all over the U.S. as a Consultant with Microsoft Services.
- Currently, I roam the "Volunteer State" as the Tennessee Technology Solution Professional for SharePoint.
- I spend most of my spare time crying about Tennessee Athletics.

[email] [Tyler.Durham@microsoft.com](mailto:Tyler.Durham@microsoft.com)

[web] <https://about.me/TNBluesBoy>



# Agenda

- Overview of Identities and Claims
- Overview of Claims in SharePoint 2010
  - [demo]::Sign In/Sign Out
- Practical Considerations
  - Claims and the Office Client
    - [demo]:: Office Client Integration
  - Claims and User Profiles
  - Claims and Search
    - [demo]::User Profiles and Search
- Additional Considerations
- Conclusion
  - Q&A

[scenario]::Collaborative Extranets

[focus]::Architects, IT Pros, Developers

# The Basics:



## Claims AuthN Overview

# Benefits of Claims AuthN

- Flexibility
  - Wide Support
  - Standards Based
- Single Sign On
  - Another Option Besides Kerberos
- Identity Federation
  - Organizations can get out of the Identity Management Business for Partners, Vendors, etc.
  - **Interesting Possibilities:** Facebook, Live, Google, etc.

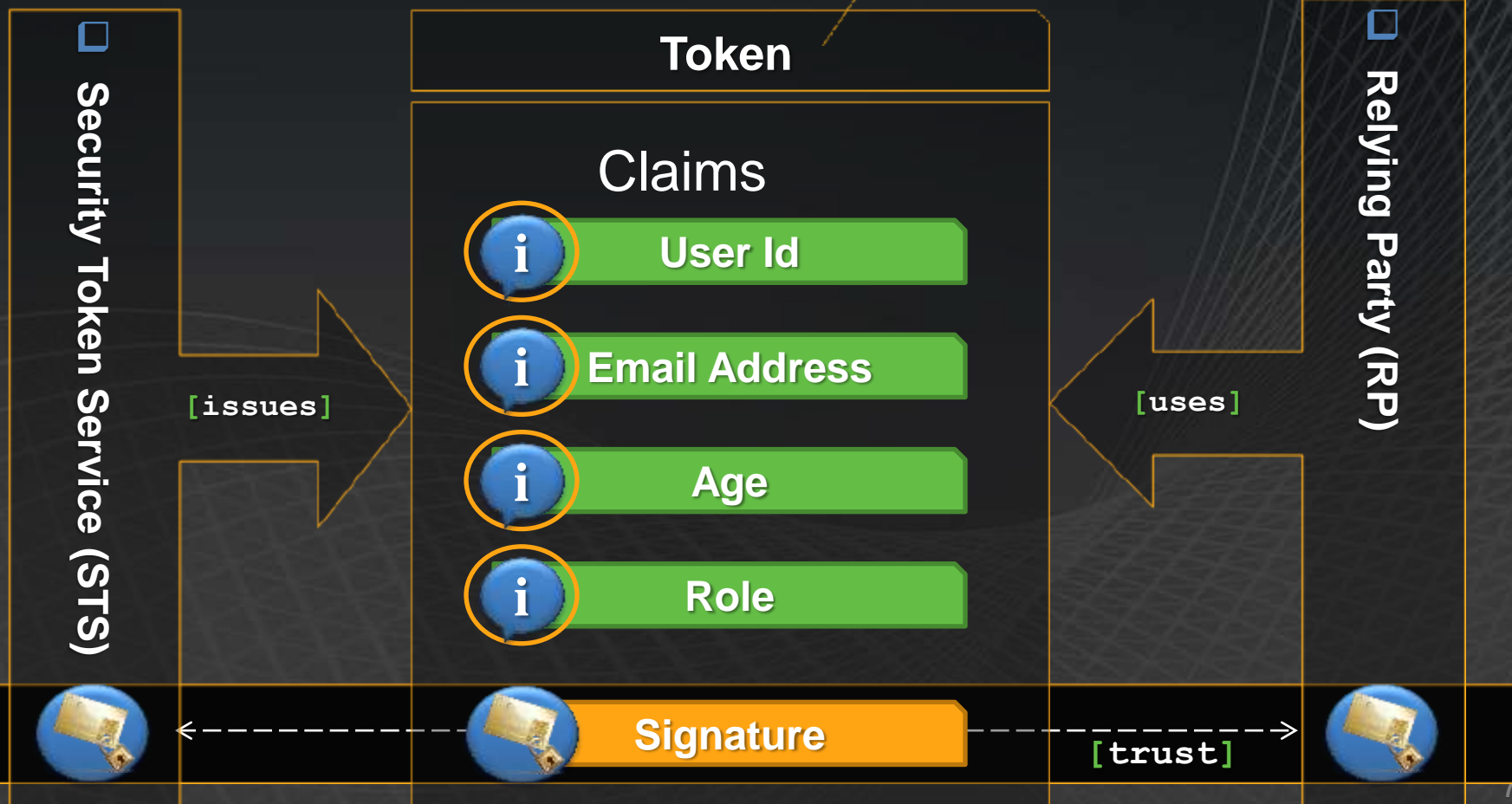
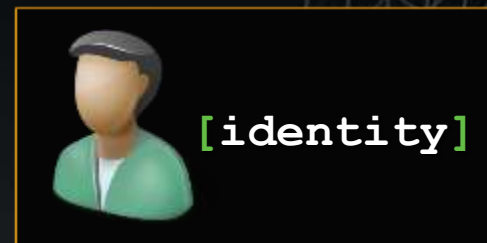
# Terminology & Concepts

- Identity
  - Information about a Person or Object (i.e.: a **User**)
  - You probably have a few: **Active Directory**, **Google**, **Windows Live**, **FaceBook**, etc.
- Claim
  - Attributes about an Identity: User ID, Email Address, Age, etc.
- Token
  - Binary Representation of an Identity
  - Set of Claims + Signature
- Relying Party (RP)
  - Uses Tokens for **AuthN** & **AuthZ**
  - In this case, SP 2010 is an RP
- Secure Token Service (STS)
  - AuthN's a User &
  - Issues Tokens for the User

↑  
[trust]  
↓



# Identities, Tokens, and Claims



# Claims AuthN Toolbox



- Windows PowerShell
  - STSADM is **Depracated!**
  - Load the **Microsoft.SharePoint.PowerShell** Snap-In
- OR**
- Run the SharePoint 2010 Management Shell
- Fiddler (HTTP/Web Debugging Proxy)
  - <http://www.fiddler2.com/fiddler2/>
- Claims Viewer Web Part
- Secure Token Service
  - Commercial (ADFS 2.0, PingFederate, etc.)
  - Write your Own using Windows Identity Framework SDK
  - SelfSTS

# SharePoint and Claims



## Overview & Architecture

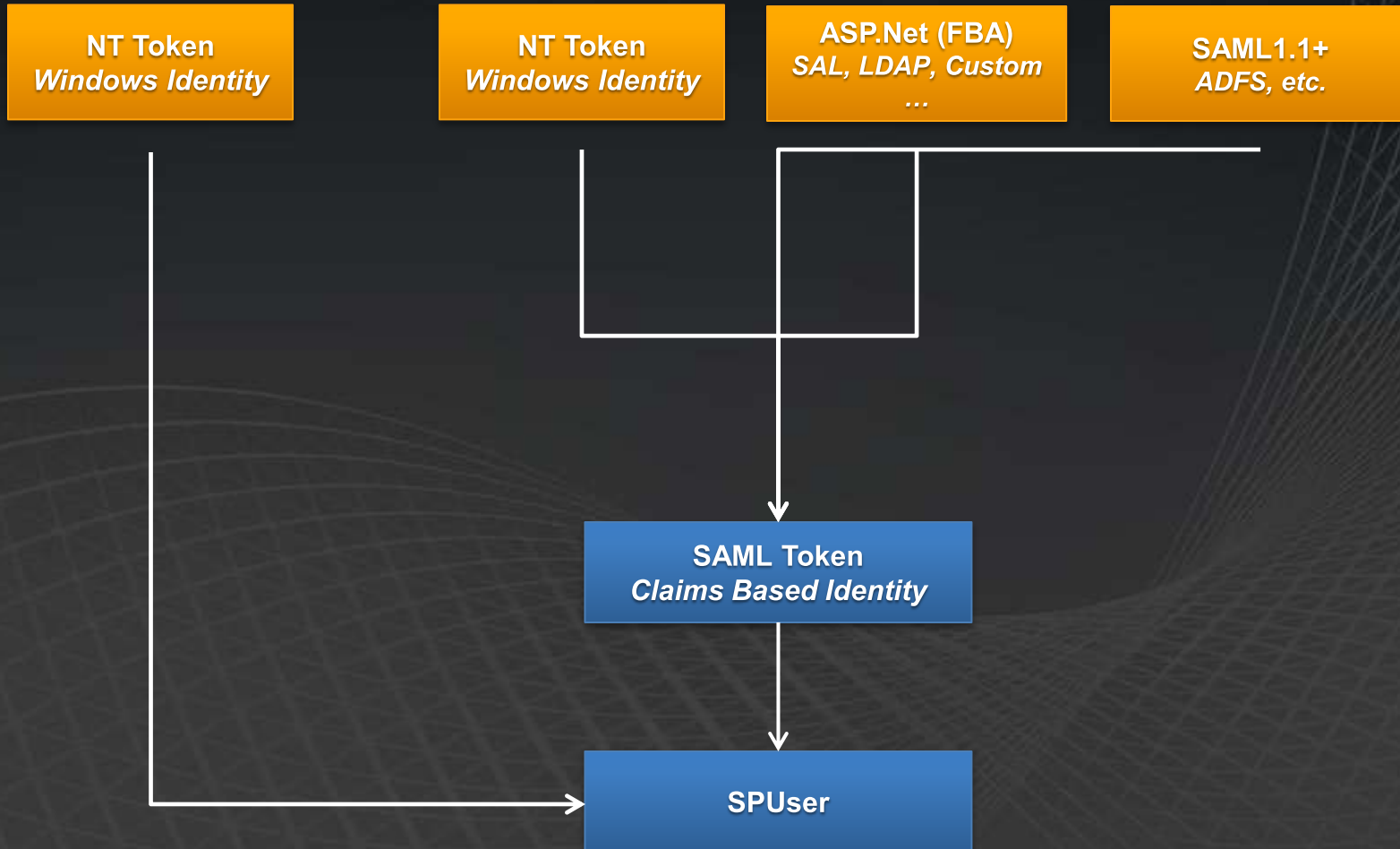
# Goals and Driving Principles

- Faciliate AuthN Externalization
  - Windows, Forms Based (SQL, LDAP, etc.), and SAML 1.1 AuthN
- Identity Normalization
  - Roll Up to SPUser
- Support Existing Infrastructure
  - “Mixed-Mode” Scenarios
- Support for Standards
  - WS-Federation 1.1
    - *Passive*: Browser Based
  - WS-Trust 1.4
  - SAML Token 1.1

# Identity Normalization

[classic]

[claims]



# How Claims are Used

- User Authentication
  - Who are You?
- User Authorization
  - What are You Allowed to Do?
  - **Example:** Role=Manager
- Intra-Farm Communication
  - Bypass Machine “Double Hop” Limitations of NTLM
- Inter-Farm Communication
  - Service Application Connections

# Classic AuthN Architecture

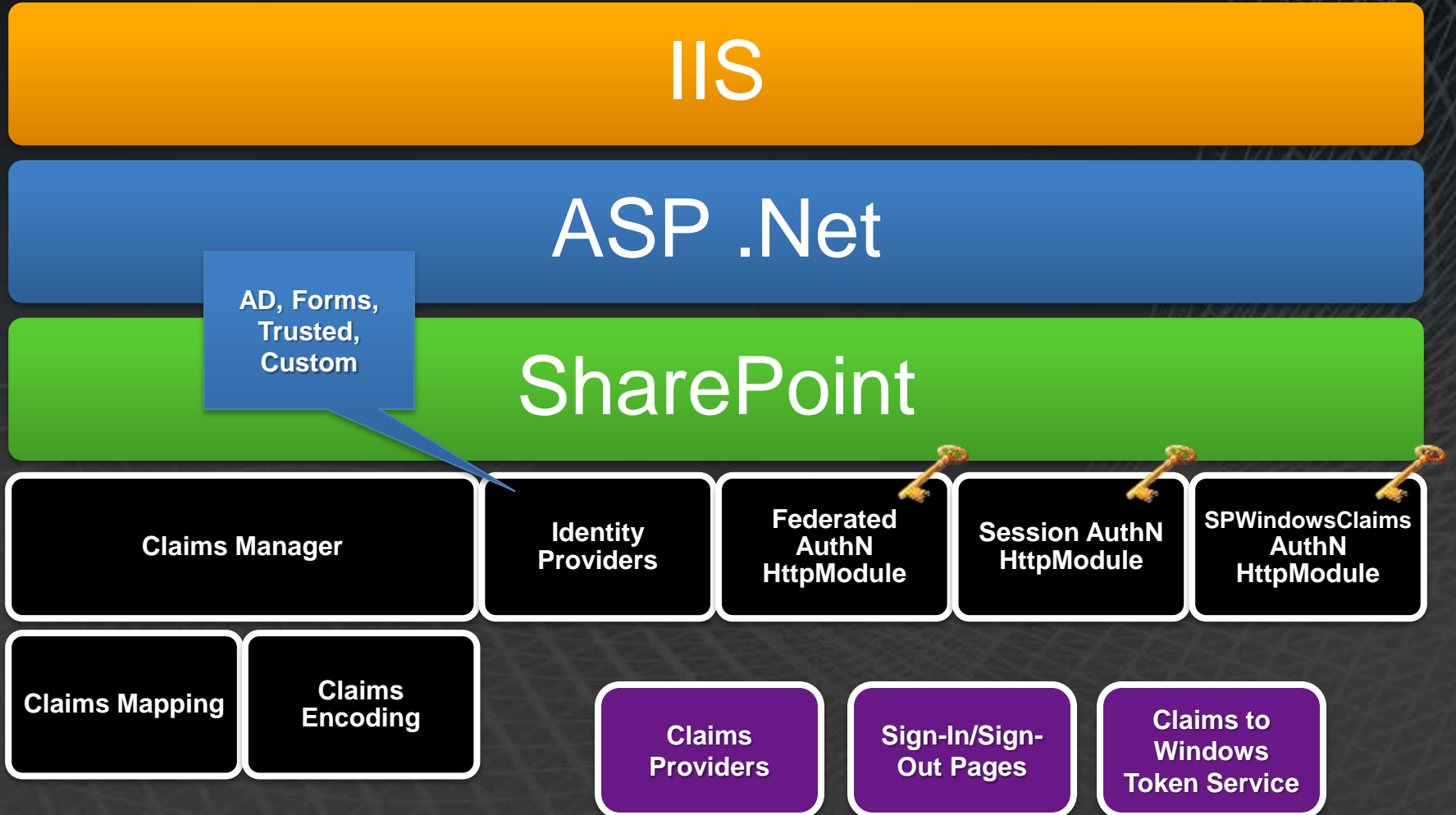
IIS

ASP .Net

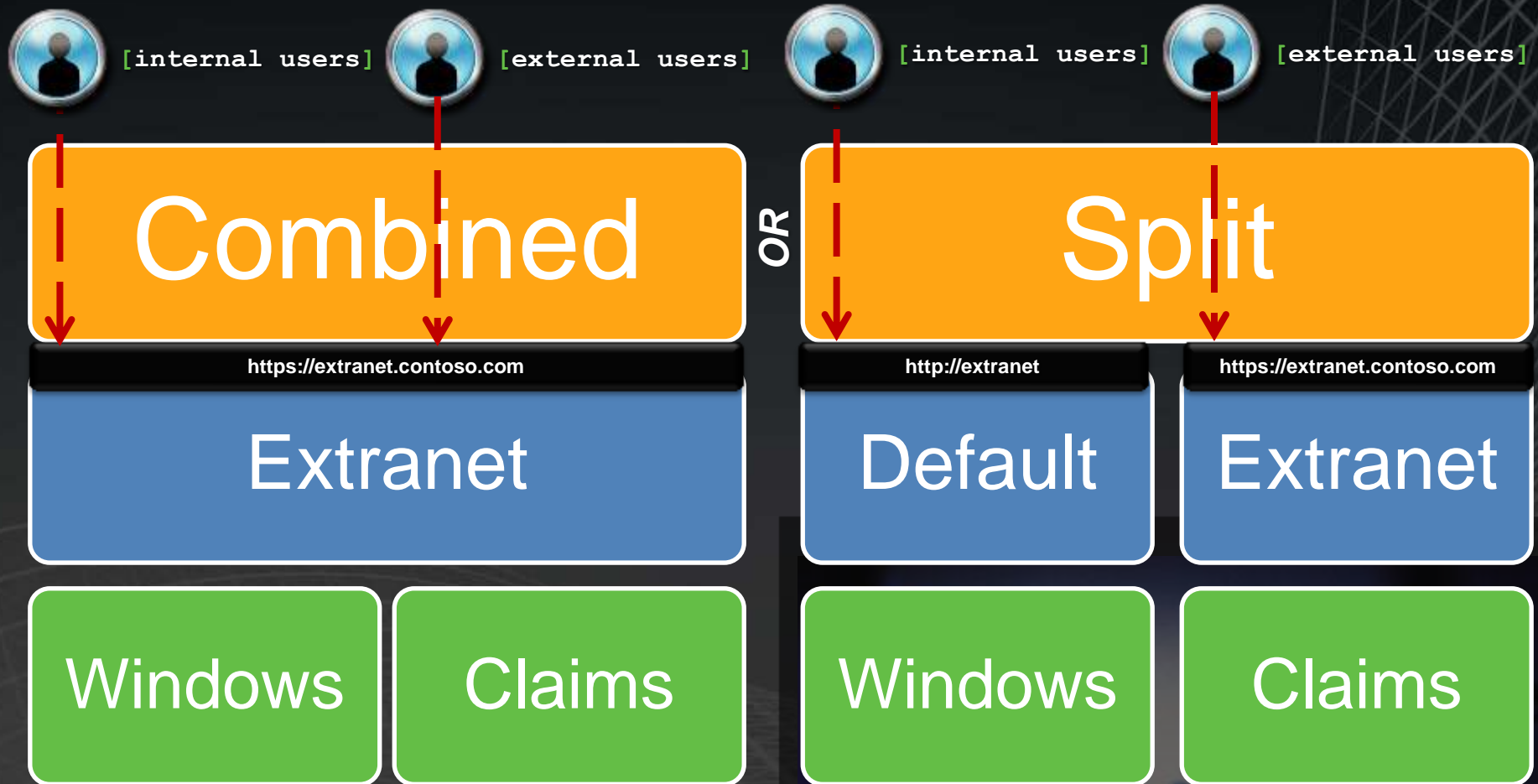
Authentication (HttpModules)

SharePoint

# Claims AuthN Architecture



# Ref. Architecture: Claims and Zones



[new in 2010]::Multiple AuthN Providers  
in same Zone!

# Setup Overview

1

### Establish Trust

- Export Token Signing Cert. from STS
- Import Token Signing Cert. into SharePoint

PowerShell or  
Central Admin

2

### Configure Trusted Token Provider

- Set Signing Cert.
- Set Sign-In URL
- Set Claims Mappings
- Important: Identity Claim
- Set Realm

PowerShell

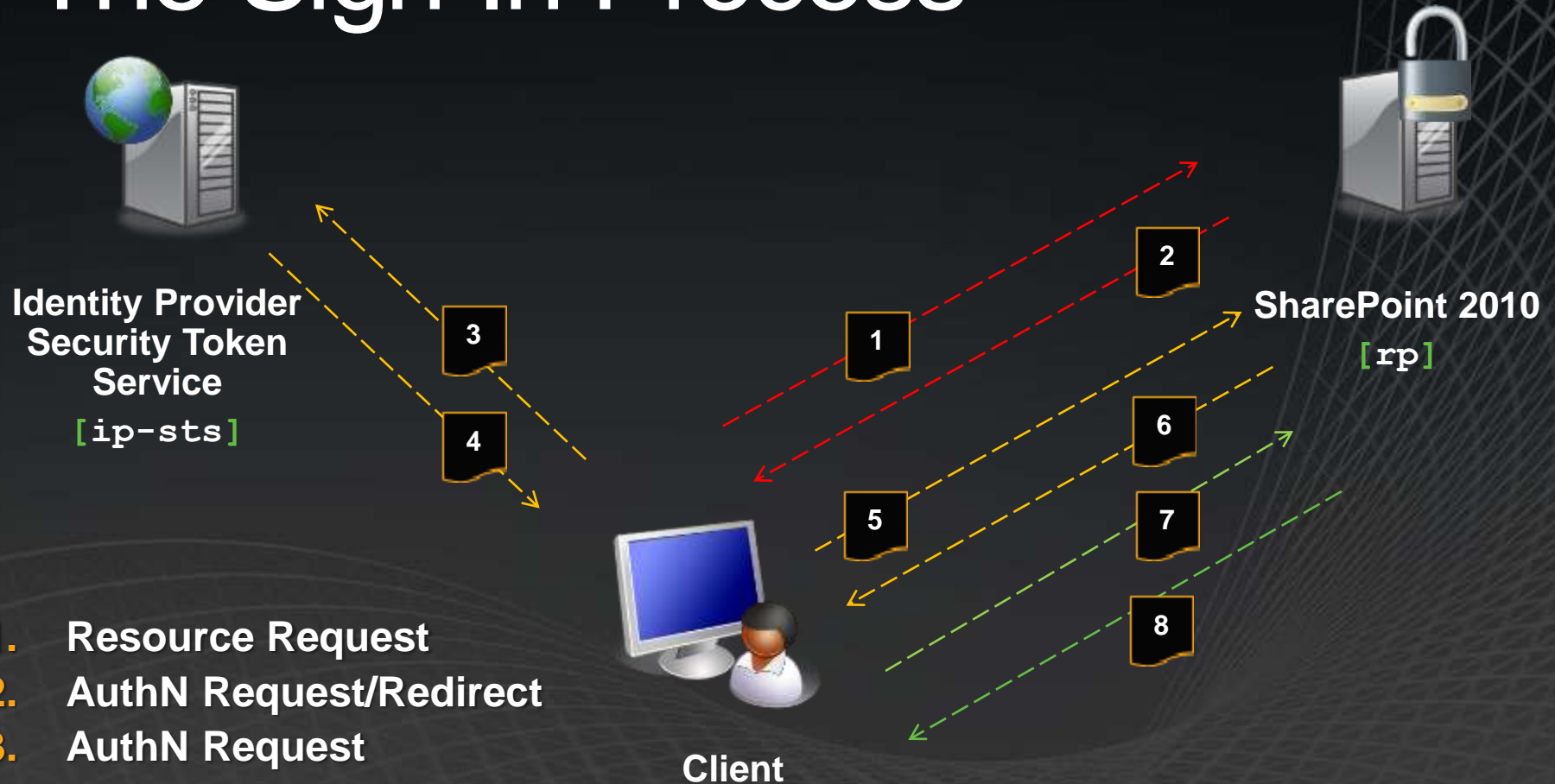
3

### Configure the Web Application

- Bind to Trusted Token Provider
- [optional] Configure Custom Login Page

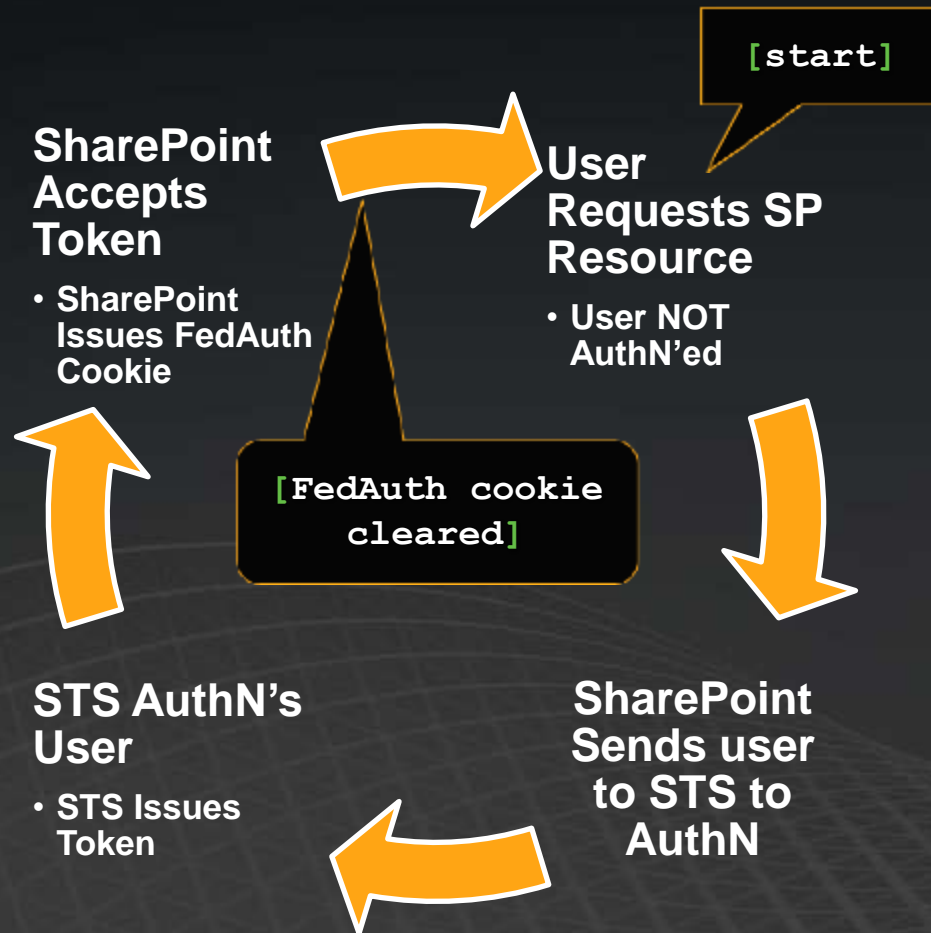
PowerShell or  
Central Admin

# The Sign-In Process



1. Resource Request
2. AuthN Request/Redirect
3. AuthN Request
4. Security Token
5. Service Token Request
6. Service Token
7. Resource Request w/Service Token
8. Resource Sent

## Stuck in “Endless” AuthN Loop



- **Symptom**
  - Always End up on SP Login Page
- **Cause**
  - Token Expiration is > SharePoint Token Cache Expiration
  - SharePoint is Clearing the “AuthN” Cookie
- **Resolution**
  - Ensure the Token Expiration is <= SharePoint Token Cache Expiration
  - Configure in PowerShell

[tip] :: See “[Setting the Login Token Expiration Correctly for SharePoint 2010 SAML Claims Users](#)” for more information.



# Demo

## Sign-In/Sign-Out



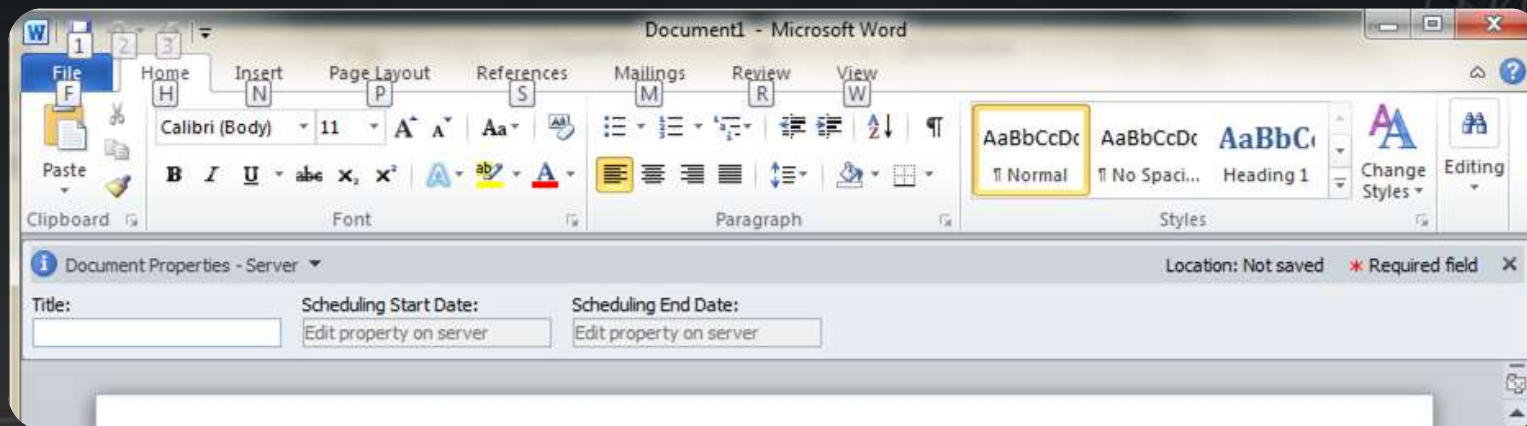
# SharePoint 2010, Claims, and the Office Client

# Overview

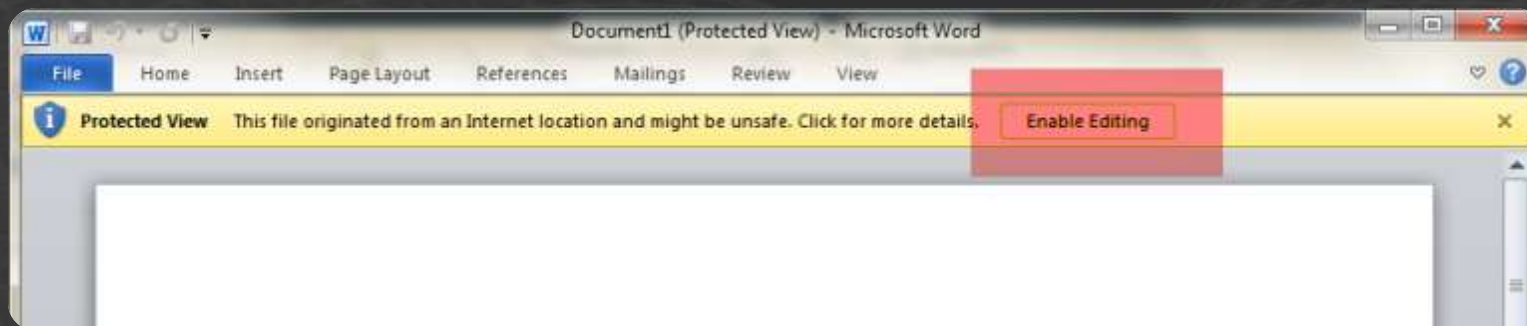
- Same Experience as in the Browser
  - Check In/Check Out
  - Start Workflows
  - Integrated Calendars, Tasks, etc.
- Supported Office Clients:
  - Office 2010
  - Office 2007 SP2
- Considerations
  - Sites in the IE “Trusted” Zone
  - To use/not use Session Cookies?

# Impact of Trusted Sites

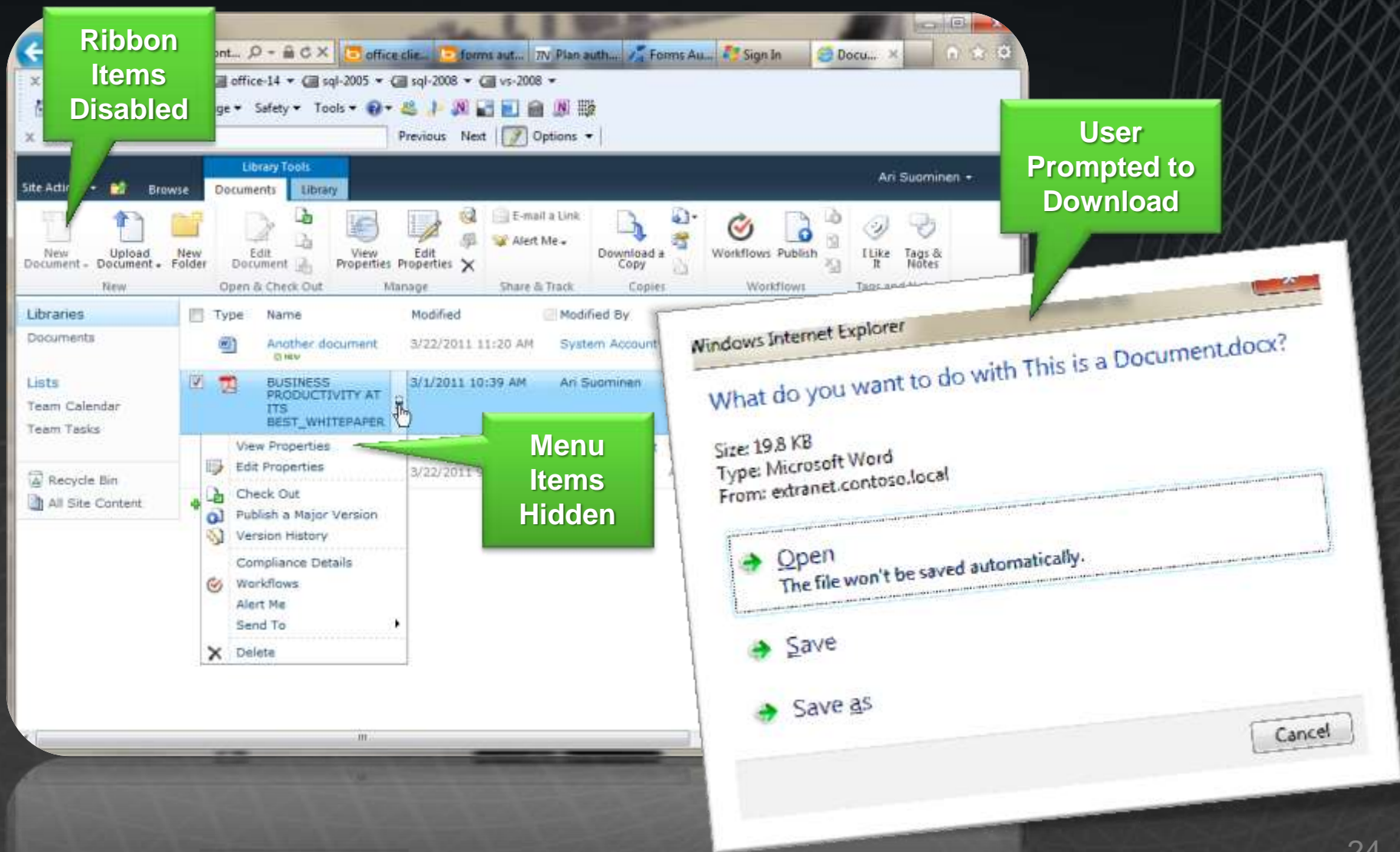
## URL in IE Trusted Sites:



## URL **NOT** in IE Trusted Sites:



# Disabling Client Integration





# Demo

SharePoint, Claims, and the Office Client

# SharePoint and Service Applications



**User Profiles,  
Search,  
Etc.**

# Claims and User Profiles

- Import Considerations
  - Additional Config. Info Required
  - Supported Directories
    - Active Directory
    - Novell eDirectory version 8.7.3
    - Sun Java System Directory Server version 5.2
    - IBM Tivoli version 5.2
    - AD LDS, etc. using LDIF Workaround
- Identity Claims are Encoded
  - Applications Need to be Aware of this
- Consider My Sites Host on Same Web Application
  - Avoids having to re-authenticate
  - Not a good idea if you plan to use Personal Sites

# SharePoint and User Profiles

## Configuring Import

### Connection Settings

Specify the Type of AuthN Provider

Specify the Specific Trusted Provider

- Similar to Configuring User Profiles for a Directory
- Imported User IDs will be “Claims Encoded”

### Profile Property Settings

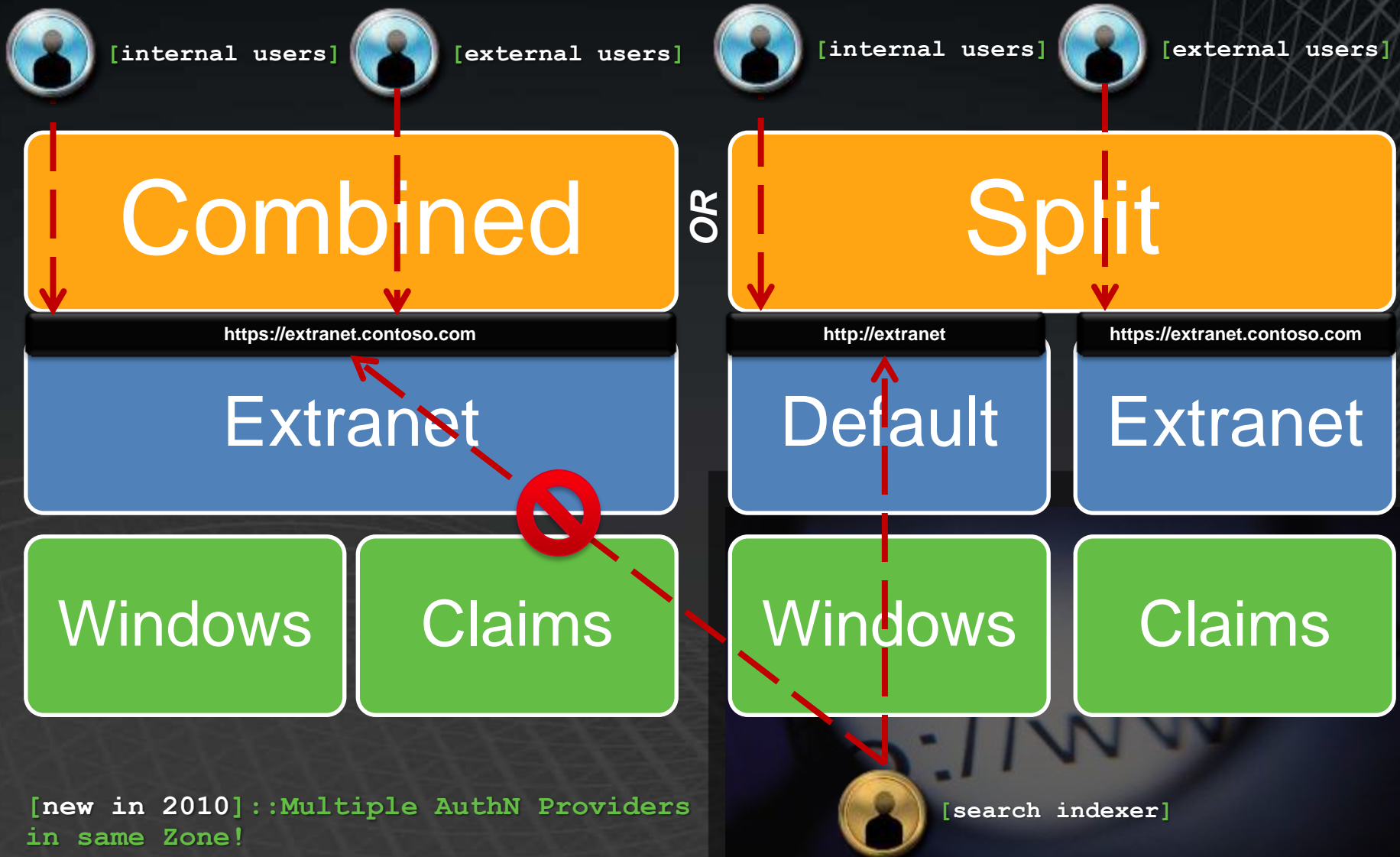
Property Name	Value
Claim User Identifier	mail

Map “Claim User Identifier” Property to the Configured Identity Claim

# Claims Encoding

- Prefixed with a value that allows SharePoint to reference the Identity Token Provider that issued the Claim
- `[example]::i:0#.w|contoso\johnsmith`
- `[example]::i:0#.w|johnsmith@contoso.com`
- Use SPClaimProviderManager to Encode/Decode
  - `EncodeClaim()`
  - `DecodeClaim()`

# Claims and Zones... & Search!



[new in 2010]::Multiple AuthN Providers in same Zone!

 Important: Indexer Needs a Windows Zone!



# Demo

## SharePoint User Profiles & Search

# Additional Considerations

- SharePoint Designer
  - Does not support working with Claims Enabled Endpoints for Web Services
  - See KB [982268](#)
- People Picker
  - Resolve & Validate Identities
  - You may Consider Creating a Custom Claim Provider
- Upgrade - Claims or Classic?
  - If Claims, you will need to”
    - Migrate Users
    - Test & Re-Work Customizations (Web Parts, etc.)

# Claims Viewer Web Part (Source Code)

```
[ToolboxItemAttribute(false)]
public class ClaimsViewerWebPart : WebPart
{
    protected override void CreateChildControls()
    {
        var claimsPrincipal = Page.User as IClaimsPrincipal;

        if(claimsPrincipal != null)
        {
            var claimsIdentity = claimsPrincipal.Identity as IClaimsIdentity;
            var gridView = new GridView();
            gridView.DataSource = claimsIdentity.Claims;

            Controls.Add(gridView);
        }
    }

    protected override void OnPreRender(EventArgs e)
    {
        base.OnPreRender(e);

        DataBind();
    }
}
```





**Microsoft**<sup>®</sup>

*Your potential. Our passion.*<sup>™</sup>

© 2010 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. 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 provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.