

# Access By Federation for Client Collaboration

INFO 1



# Introduction

- ◆ Holly Hanna, Microsoft Legal & Corporate Affairs  
[hollyhan@microsoft.com](mailto:hollyhan@microsoft.com)  
@hollyhanna (Twitter)
- ◆ Karen Allen, Morgan Lewis & Bockius  
[kallen@morganlewis.com](mailto:kallen@morganlewis.com)

# Authentication Issues - Fundamental Questions

- ◆ Authentication: “Who are you?”
- ◆ Authorization: “Are you allowed to do this?”
- ◆ AD Accounts - secure but a management nightmare
- ◆ Forms-based - easier to implement, but less secure

# Microsoft Yesterday: Two Options, Neither Good



# Option 1: Extranet

- ◆ Requires user to be set up in PARTNER domain
- ◆ Passwords need to be updated every 70 days
- ◆ Environment running on SharePoint 2007 - no way to collaborate in real time
- ◆ Management a constant headache for both administrator and user

# Option 2: CorpNet Account

- ◆ 2+ week process for getting users set up in the system
- ◆ To remotely access the corporate network, external users must be approved for a smart card, requiring director-level approval
- ◆ Once remote access is approved, user must either visit a Microsoft location or send in picture and get a card mailed
- ◆ Once the user has access, they have access to the entire Microsoft corporate network - not just the matter they are working on

# MorganLewis Extranet

- ◆ Requires user to be set up in AD domain
  - ◆ Used to limit access to sites and externally exposed applications
- ◆ Passwords complex, need to be updated every 90 days
- ◆ Environment running on SharePoint 2007 - no way to collaborate in real time
- ◆ Management a constant for both administrator and user
- ◆ Dedicated support team for password resets and other access issues

# Circumventing the System





# IT Goal: Make It Easy

- ◆ When forced to choose between the right way to do something and the expedient way to do something, expedience wins every time
- ◆ Understand your security tradeoffs and undertake a solid risk analysis

# Claims Authentication Fundamentals

6 Point ID  
Document Selector



# Secure Authentication Options

Claims-based =  
Authoritative Identity Source

- ◆ Microsoft Account
- ◆ ADFS
- ◆ OAuth

# Microsoft Today: External Collaboration Made Easy

- ◆ External users need a Microsoft Account (formerly Live ID or Passport), which can be easily created by the end user and associated with their email address
- ◆ Site owner sends an invitation from O365 site to the associated email address

# What's a Microsoft Account?

- ◆ Single sign-on web service formerly known as Passport and Windows Live ID
- ◆ Available to anyone with an email address; automatic with a Hotmail.com or outlook.com address
- ◆ User is authenticated via SSL connection; if the user opts to have a site remember them, an encrypted time-limited cookie is stored on their computer and attached to a triple DES encrypted ID tag
- ◆ ID is sent to the web site, which then plants another time-limited HTTP cookie on the user's computer.

# 0365 External Collaboration

Office 365

Outlook



EDIT LINKS

Home ⓘ

EDIT LINKS

⚠ Please remember that this site may be shared with people outside of Microsoft. Learn more about [external sharing](#) and the [Usage Guidelines](#) for this site

Share 'LCA Sandbox' ×

⚠ **MBI:** This site can only be shared with those who have a legitimate business need, not to be disclosed publically. **This site may be shared with external users.**

Shared with Karalee Quinton (Lincoln Bay Company), Eva Lo (LCA), and Carol Corneby (RCM) (includes external users)

Invite people to 'Contribute'

Enter names, email addresses, or 'Everyone'.

Include a personal message with this invitation (Optional).

SHOW OPTIONS

Share

Cancel

Office 365

Hello,

Here's the site that Holly Hanna (LCA) shared with you.

Go To [LCA Sandbox](#)

Microsoft

Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399  
This message was sent from an unmonitored e-mail address.  
Please do not reply to this message.  
[Privacy](#) | [Legal](#)



# Securing O365 Collaboration

- ◆ Invitation is tokenized; cannot be forwarded or used by anyone who is not the intended recipient
- ◆ Link expires after one week for external users
- ◆ Only internal users can be owners and send invitations
- ◆ While individual items can be shared with non-site users by external users, site sharing is restricted to owners
- ◆ External users have access only to the sites they've been invited to and nothing else

# Yammer External Collaboration

**Microsoft - PPP Firm Engagement**

Yammer® Search for people, groups and conversations Add People Groups Files Apps Account

**Holly Hanna**  
Home  
Inbox  
GROUPS  
All Network  
Winston Strawn E...  
**Legal Executive Rou...**  
Browse Groups  
Create Group  
Networks  
Admin

**Legal Executive Roundtable - March 2013** Settings Joined  
Public Group [legalexecutiveroundtable-march2013+ppp-microsof...](#)  
This group will be used to post materials related to the Legal Executive Roundtable event in March 2013.

Conversations Info Files Notes

Share an Update Add a Doc/Image Post a Poll More  
Add Members Embed This Feed

Share something with this group...

**Holly Hanna**  
to Legal Executive Roundtable - March 2013  
Adding the eDiscovery deck from the presentation with Joe Banks and EJ Bastien.

**Wave 15 eDiscovery Presentation for PPP**  
Uploaded to Legal Executive Roundtable - March 2013  
Files  
Like Reply Stop Following More April 5 at 2:13pm  
Larry Kuhn likes this.  
Write a reply...

**Holly Hanna**  
to Legal Executive Roundtable - March 2013  
Whitepaper on "pass the hash" attacks:  
<http://download.microsoft.com/download/7/71/A/77ABC5BD-8320-4...>  
Pass-the-Hash (PtH) Attacks and Other Credential Theft

INFO  
Click here to edit this info section.

QUICK ACCESS  
POPULAR  
MS1732\_All\_Hands\_Surface\_r01  
Uploaded 4 months ago  
Wave 15 eDiscovery Presentatio...  
Uploaded 3 months ago  
RECOMMENDED  
PPPAgenda  
Uploaded 4 months ago  
Add File Note Link

RELATED GROUPS  
Add a related group...

Online Now  
Search  
Ed Empamano Director  
Dennis Garcia (LCA) SENIOR ATTORNEY  
Marjorie Wilson Senior Attorney  
John Anderson



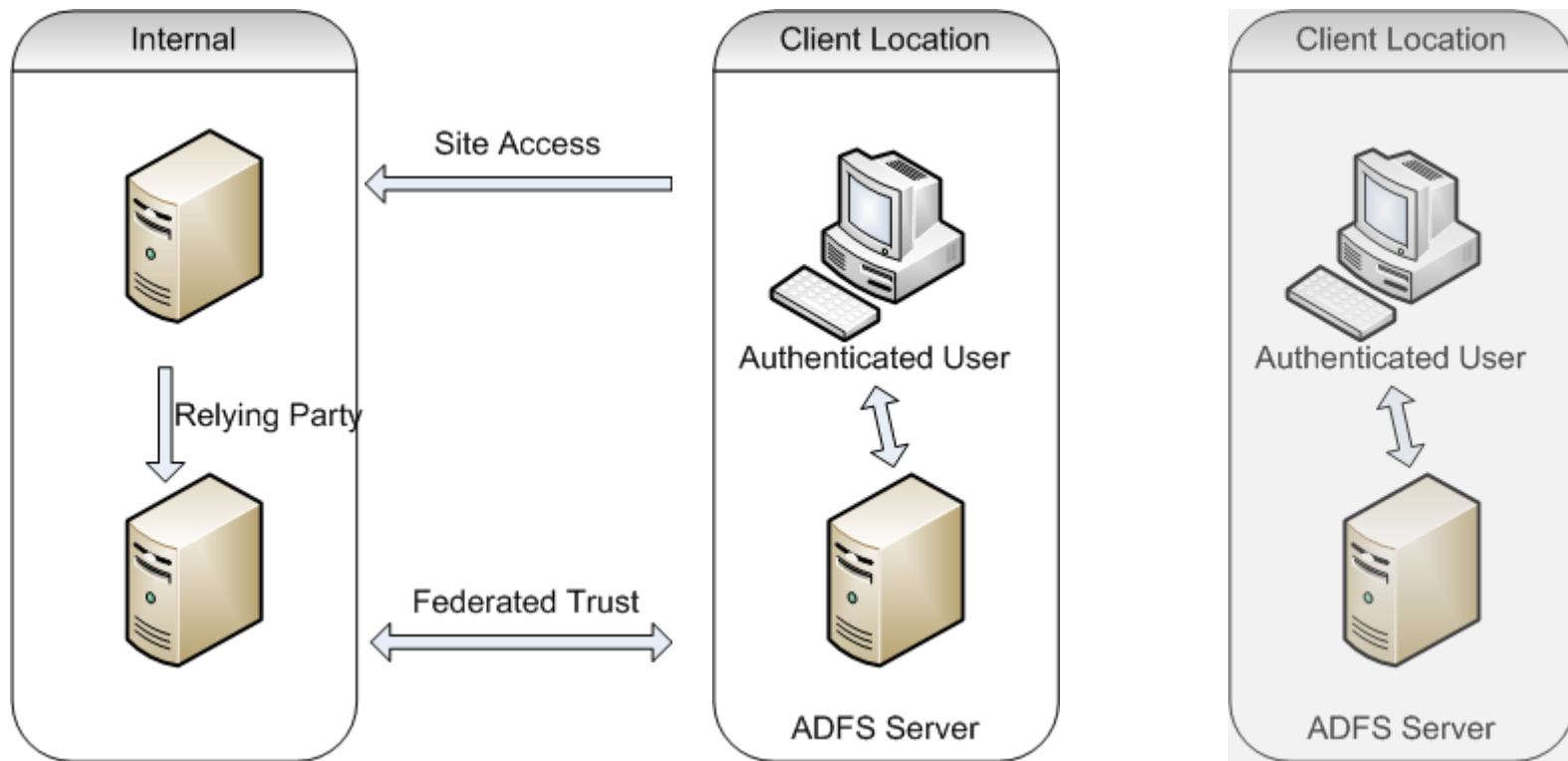


# Single Sign-On via ADFS

- ◆ Client Request for single sign-on to SharePoint extranet site
- ◆ Client's AD configured as Claims Provider
- ◆ Configured SharePoint to trust the claims coming from ADFS for authentication
- ◆ Management
  - ◆ Defined groups and roles within SharePoint to match the client's AD group name
  - ◆ Linked the groups to Policies in SharePoint
  - ◆ Group Membership in AD is managed in the client's AD
  - ◆ Allows the client to add users as necessary

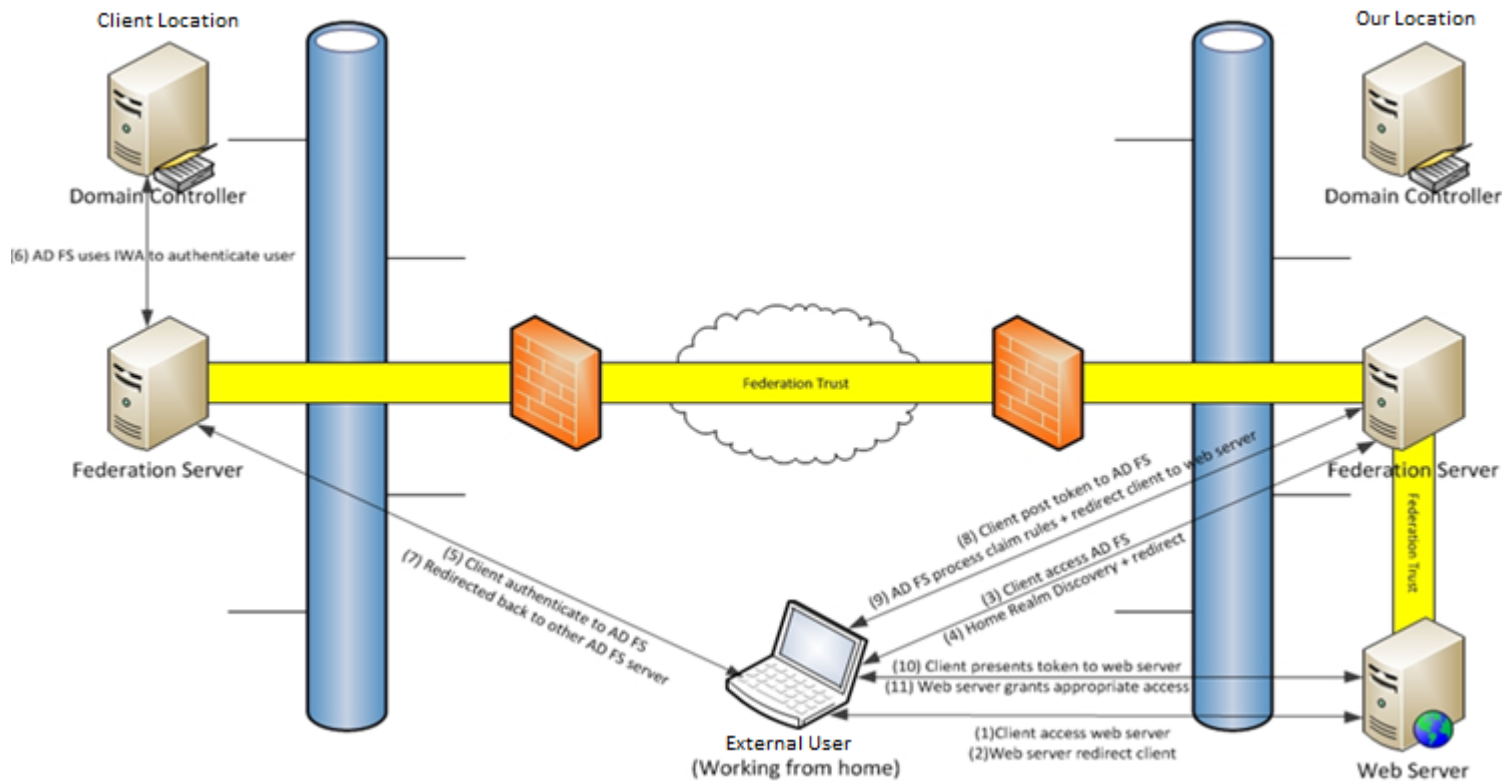
# ADFS Architecture

## Simple View



# ADFS Architecture

## Detail View



# Application Configuration

- ◆ Extend Webapp to SSL site (extranet zone)
- ◆ Requires Federation Extensions for SharePoint
- ◆ Add external groups as Roles via WebApp policy

Central Administration > Application Management > Policy for Web Application

## Policy for Web Application

[Add Users](#) | [Delete Selected Users](#) | [Edit Permissions of Selected Users](#) Web Application:

<input type="checkbox"/>	Zone	Display Name	User Name
<input type="checkbox"/>	Extranet	<a href="#">Role#Domain Users</a>	sharepointclaimsroleprovider:role#domain users
<input type="checkbox"/>	Extranet	<a href="#">Role#PortalUsers</a>	sharepointclaimsroleprovider:role#portalusers
<input type="checkbox"/>	Extranet	<a href="#">Role#OrgUnit_SL_Corporate_Morgan_Lewis_Legal</a>	sharepointclaimsroleprovider:role#orgunit_sl_corporate_morgan_lewis_legal

# Microsoft Account Pros & Cons

## ◆ Advantages

- ◆ Makes it easy for attorneys to collaborate in real time with outside counsel
- ◆ Available for any device, anywhere; offline sync to local machine
- ◆ With Windows 8, user is already signed in; when accessing a collaboration site, pass-thru of credentials is seamless

## ◆ Disadvantages

- ◆ If user's Microsoft account is compromised, shared documents could be at risk
- ◆ No IT control over who has access to what data

# ADFS Pros & Cons

## ◆ Advantages

- ◆ Shifts burden of authenticating users to the identity provider
- ◆ Vendor neutral SAML-based token
- ◆ Seamless for end users

## ◆ Disadvantages

- ◆ More complex configuration
- ◆ Support issues for end-users
  - ◆ Troubleshooting on both sides

# Coming Attractions

## Open Authentication

Strongly Authenticating Everyone, Everything, and Everywhere



- ◆ Industry Standard Protocol
- ◆ Used by Citrix FileStream, Box.com, Windows Live, and others

# Further Reading

- ◆ Claims-Based Identity Term Definitions  
<http://msdn.microsoft.com/en-us/library/ee534975.aspx>
- ◆ Open Authentication (OAuth) Overview  
<http://en.wikipedia.org/wiki/OAuth>
- ◆ Microsoft Account  
<https://signup.live.com>
- ◆ ADFS Concepts  
[http://technet.microsoft.com/en-us/library/cc776617\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc776617(v=ws.10).aspx)