IDA314 – Live ID, Open ID & OAuth

What is the difference between them?

Jorgen Thelin, Windows Live Identity Services

Microsoft Confidential

Agenda

- Online Identity 101
- What is Open ID?
- What is OAuth?
- What is Live ID?
- Compare and contrast

Microsoft Confidential

Online Identity 101

- Digital identity is "a set of claims made by one digital subject about itself or another digital subject" -- Kim Cameron
  - User view: Who you are, how you prove it, & what that permits you to do
- Why do people care about online identity ?
  - Too many accounts
  - Too many credentials
  - Barriers to collaboration - Re-authenticate to access new resources
  - Good authentication is secure but unobtrusive
    - But there too many bad authentication experiences in current applications and services
    - Bad UX leads to weak security - password fatigue, "Post-it passwords", etc
- What is "federated identity" ?
  - "Identity without borders"
  - User's sign in once with their Identity Provider then can seamlessly work with trusted partners

Microsoft Confidential

What is Open ID?

In their own words (http://openid.net/)

“Open ID is a free and easy way to use a single digital identity across the Internet.”

TechReady 7

What is Open ID?

- A Web single-sign-on solution
- A personal identifier (OpenID URI)
- An authentication protocol
- A standards organization
- A business model

Microsoft Confidential

What Open ID Isn't

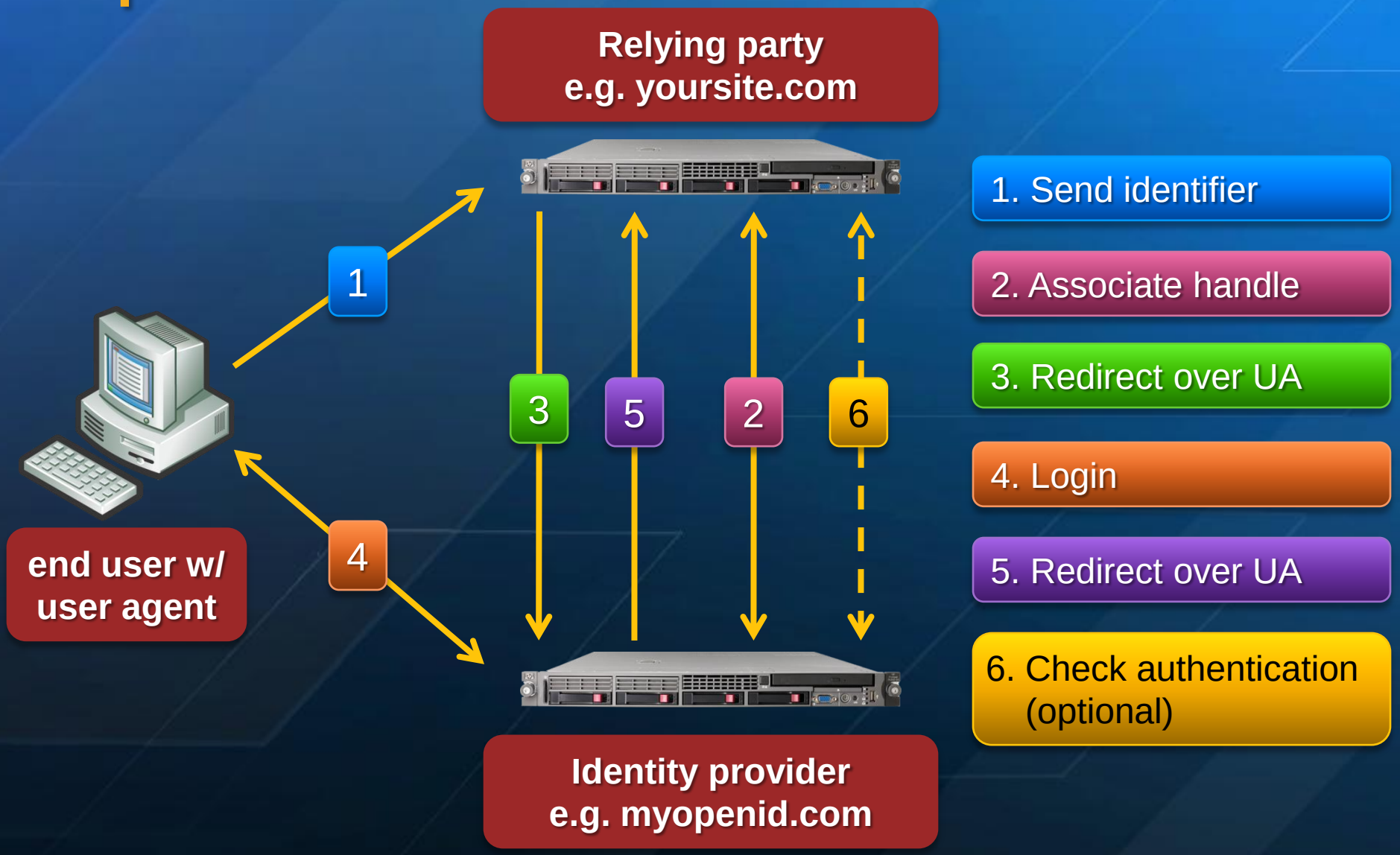
- Not an Identity Provider – there are many
- Not an account, just an identity
  - User still need to register with each new site
- Not a guarantee of anything except the user's URI
- Not a trust broker – "*Identity is not Trust!*"

Microsoft Confidential

Demo – Open ID Authentication

TechReady 7

OpenID Protocol Mechanics



+ IP-Delegation + Discovery Functionality in Open ID 2.0

Microsoft Confidential

Who's Using OpenID?

Identity Providers

Relying Parties

- Provider lists:
  - OpenID Directory
- Adopter lists:
  - OpenID.net, MyOpenID, OpenID Directory, ClickPass

Microsoft Confidential

Considerations for Relying Parties

- RPs are placing trust in the Open ID providers they accept (providers can be the weak link)
  - Provider security levels are paramount and not standardized
- Low-value web sites happy to accept any OpenID provider
- High-value web properties are rightly much more selective on which Open ID providers they trust
  - **HealthVault** only accepts VeriSign or TrustBearer
  - AOL has white-listed 15 providers
- White-listing of providers is becoming the norm, but without standards
- Open ID can be a spammers dream (lots of IDs)

Microsoft Confidential

Open ID - User Experience

User experience is generally holding back widespread adoption

- Open ID identity is a URI
  - Good for Geeks; Bad for Grandmas
- Open ID URL raises some privacy concerns because of cross-site account correlation
- Little progress on mobile friendly Open ID experience
- Open ID protocol can be prone to hacking
- Pain if Open ID provider disappears / goes down – 99.999% availability is HARD WORK!

Microsoft Confidential

Summary - Open ID

- Open ID provides
  - Single-sign-on through a standard authentication protocol
  - More benefit to new websites (relying parties) than established ones
- High-value sites need to be selective about which providers they accept / trust.
  - http://openid.spammer.com is bad!
- Main challenge remains
  - Ease-of-use (for users)
  - Trust relationships (for relying parties)

Microsoft Confidential

What is OAuth?

In their own words (http://oauth.net/)

"An open protocol to allow secure API authentication in a simple and standard method from desktop and web applications."

What is OAuth?

- An application authentication protocol
- An application authorization protocol for user consent to data sharing
- Attempt at convergence for authentication / authorization protocol for all major use cases (web, mobile, smart client)
- Developed by an informal community group

and many others…

Microsoft Confidential

What OAuth Isn't

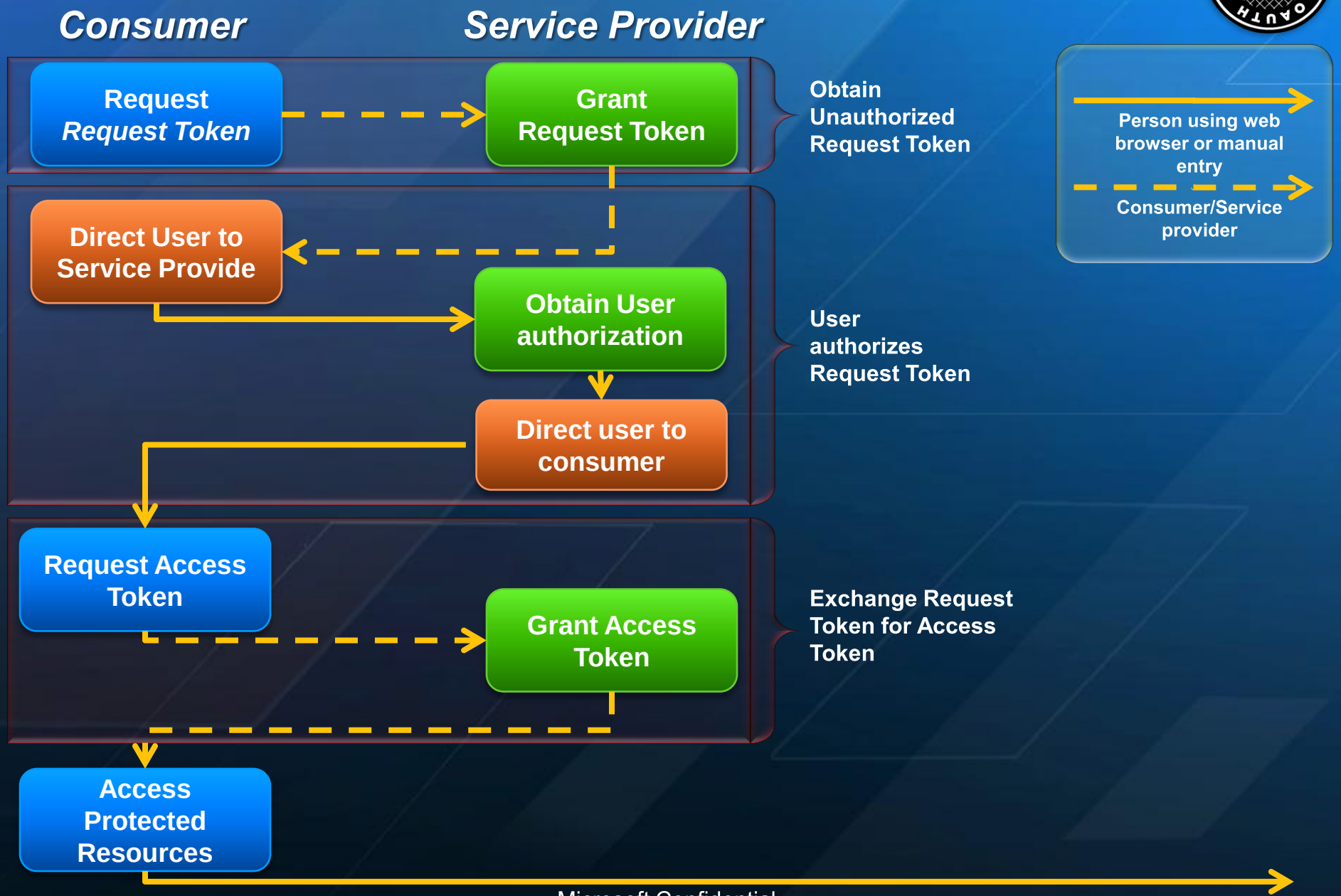
- Not related to OpenID – except for a shared ‘O’
- Not a new concept (AuthSub, BBAuth, OpenAuth, DelAuth)
- Not yet a very clear IPR policy – in progress
- Not tied to a specific authentication mechanism
- Not a specific UX – different experience per provider
- Currently not very scalable or suited to mobile apps (verbose, chatty, lacking lifetime/refresh features)

Microsoft Confidential

Demo – OAuth Authorization

TechReady 7

OAuth Protocol Mechanics



Who's Using OAuth?

Google

YAHOO!

myspace.com

AOL

plaxo

SmugMug

flickr LOVES YOU

photobucket

magnolia

GET SATISFACTION

Pownce
Send stuff to your friends.

- Various open source client libraries available

Microsoft Confidential

Summary - OAuth

- Enables data portability through a standard authorization protocol
- Gaining rapid adoption among service providers (big and small)
- Challenges
  - Protocol scalability
  - IPR / governance ambiguity

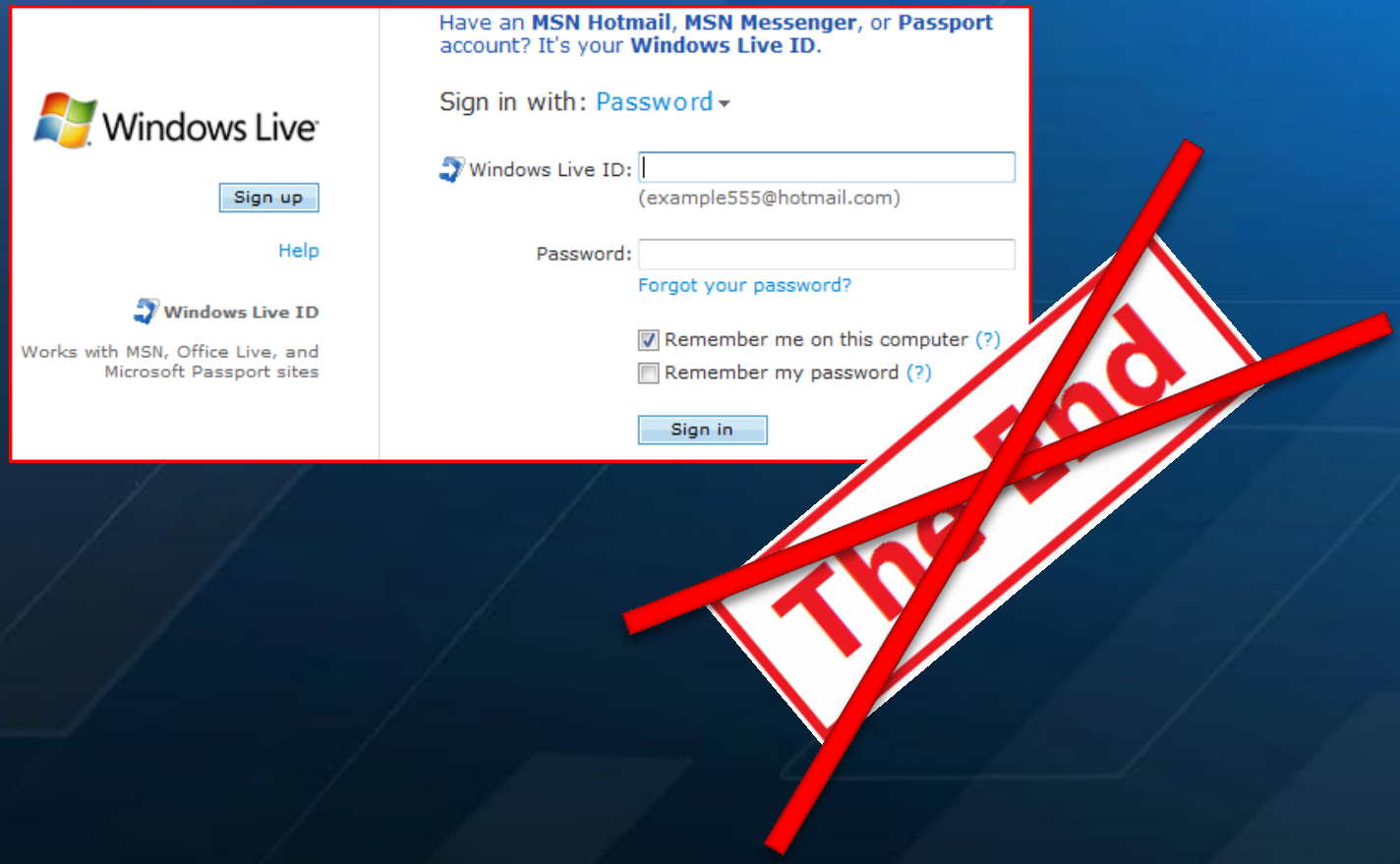
Microsoft Confidential

What is Live ID?

In their own words (http://dev.live.com/liveid/)

"Windows Live ID is the
identity and authentication system
for Microsoft services and its partners"

What is Windows Live ID?



Microsoft Confidential

What is Windows Live ID?

… the biggest authentication provider on the planet!

- ~ 500 million Active Accounts @ Jun 2008
- 200 countries, 35 languages
- ~ 1.2 billion Authentications per day
- Peak traffic is generally 2X normal load
- >~ 99.99% service availability
- > 1 million new accounts created per day
  – a huge number are by spammers ☹

Microsoft Confidential

What is Windows Live ID? (cont)

- The authentication provider for all Microsoft's web properties
- But also an identity platform:
  - An authentication platform
  - A delegation platform
  - A federation platform
  - A user and service provisioning platform
  - The first line of anti-spam defense
- All delivered as Software + Services
  - Cloud hosted + client SDK libraries
  - Two major Live ID feature releases per year

Microsoft Confidential

Live ID - Types of Identities

Principals

- User (WLID)
- Machine (Device ID)
- Machine on behalf of User (linked device)
- App (App ID)
- App on behalf of User (Delegation)

Types of WLIDs

- Passport Account, Hotmail account
- EASI (Email as Sign-In) account
- Managed namespaces
- Federated Accounts

Microsoft Confidential

Live ID - High Level Architecture

Consumers

Browsers
Internet Explorer, Firefox, Safari

Applications
Messenger, Office, Outlook Express, 3rd Party APPS

Windows Live ID Client SDK

Devices
Xbox, MSN TV, phones, pagers

Services

Web Services
mail.live.com, messenger.live.com

Windows Live ID Server SDK

Identity Owners
Personal Domains, ISPs, businesses…

Windows Live ID interface (HTTP, SOAP, TCP/IP)

Windows Live ID Service

- **Registration**
- **Authentication**
- **Authorization**
- **Account Services**
- **Parental Controls**
- **Trust Provisioning**

Federated Identity Authorities

ADFS Servers, Security Token Services speaking WS-Trust

Microsoft Confidential

Demo – Live ID Web Authentication

Web Auth Protocol Mechanics

end user w/ user agent

Relying party
e.g. yoursite.com

Windows Live ID service

Microsoft Confidential

Demo – Live ID Delegated Auth

DelAuth Protocol Mechanics

end user w/ user agent

Application Provider (web site)

Granting consent phase (must be online)

Direct user to consent UI

Receive consent token

Consent UI (consent.live.com)

"Using Consent" Phase (user can be offline)

Send delegation token with API call to resource

Receive data

Resource Provider (e.g. Windows Live Contacts)

Send refresh token

Receive new consent token

Windows Live ID Delegation Service

Microsoft Confidential

Live ID - Integration SDKs

- Smart client applications

Live ID Client SDK

- Depth partners web site integration
- Runs on Windows Server OS

Relying Party Suite (RPS – aka Live ID Server SDK)

- Breadth partners web site integration
- Open source samples in 6 languages – ASP.NET (C# & VB), Java, Perl, PHP, Ruby, Python

Web Authentication SDK (WebAuth)

- Third-party application providers access to Windows Live user's data
- Open source samples in 6 languages – ASP.NET (C# & VB), Java, Perl, PHP, Ruby, Python

Delegated Authentication SDK (DelAuth)

- Includes ASP.NET controls to simplify integration with Live ID / Windows Live:
  - Contacts, IDLogin, IDLoginView, SilverlightStreamingMedia

Windows Live Tools for Visual Studio

Microsoft Confidential

Windows Live ID Federation & Provisioning

Enabling the enterprise…

TechReady 7

Why Federate?

- Organizations can collaborate without creating or managing lots of new accounts
- Partners can include Live Services in their offerings to customer – for example hosted e-mail
- Benefits:
  - For users – smooth single sign-on (SSO) experience
  - For organizations – offer wider range of services to their users at reduced cost

Microsoft Confidential

Federated Authentication Flow

Step 1 (Partner Sign-in)

A user sends credentials to the federated partner identity provider. The federated partner's *Security Token Service (STS)* generates an IP token and returns it to the user.

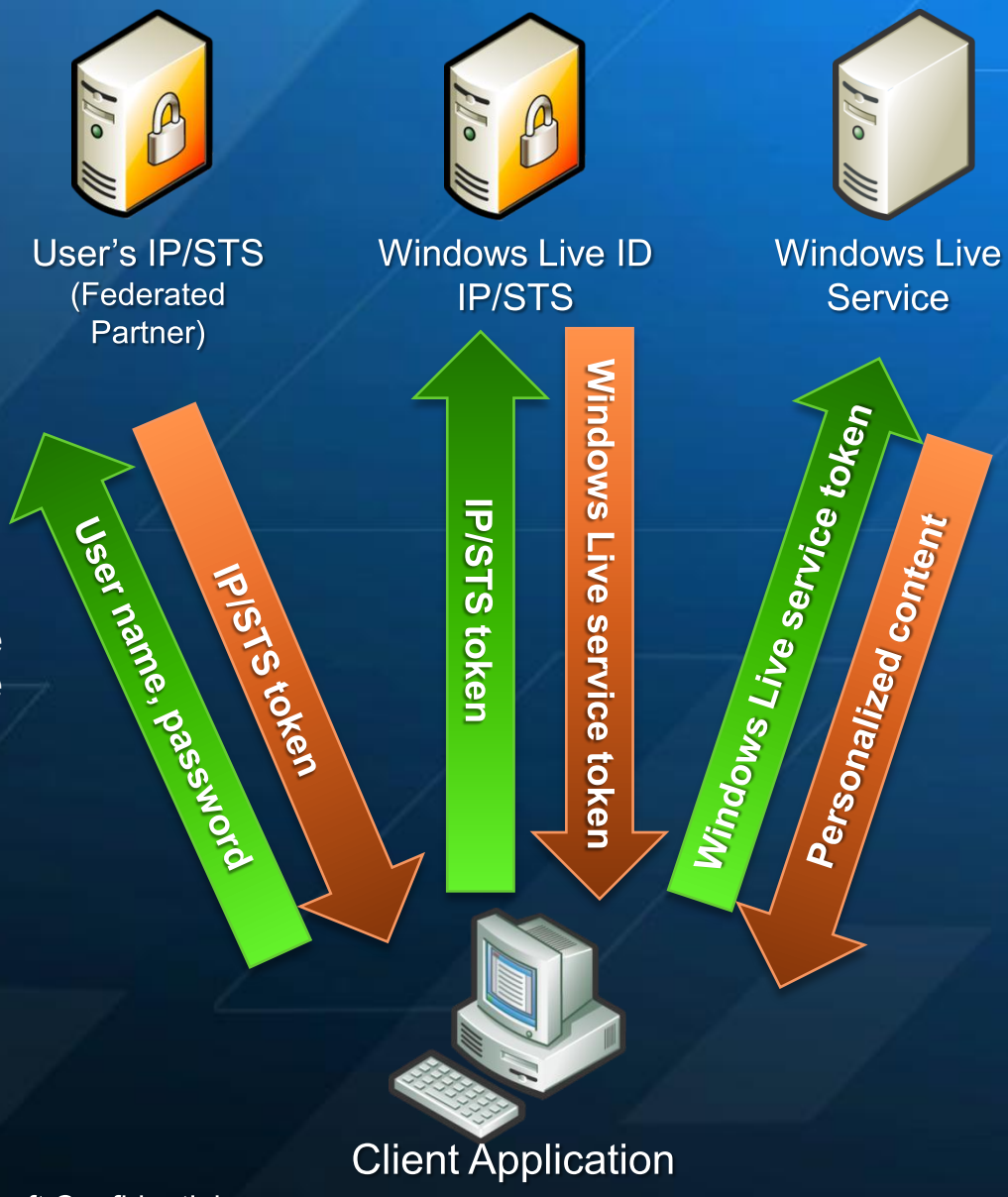
Step 2 (Windows Live ID Sign-in)

IP token is sent to Windows Live ID.
Windows Live ID STS converts the token from the federated partner to a Windows Live service token.

On the user's first visit, the Windows Live ID service maps the federated user account to a Windows Live ID unique identifier (PUID) and shadow account.

Step 3 (Service Sign-in)

The issued service token is sent to the Windows Live service that the user originally wanted to access.



Microsoft Confidential

Federation Overview

- Federation is a unidirectional or bidirectional trust relationship between organizations
  - Authentication assertions from one organization recognized by the other
  - Federation involves two parties:
    - **Identity Provider** (IP) authenticates users' identity accounts
    - **Resource Provider** or Relying Party (RP) permits access to resources in their network
- Based on WS-* standards – especially WS-Federation / WS-Trust
- Easy partner on-boarding is more than just standard protocols
  - Squatters, account merge, trust provisioning, realm discovery UX
- Shadow account creation makes federation invisible to Microsoft services

Microsoft Confidential

Service Provisioning Framework

- Problem
  - Incrementally provision specific services for a user (e.g. pre-create an inbox)
- Solution
  - SPF – Service Provisioning Framework
  - Scalable system to 100s of millions of users
  - Fully data driven to reconfigure service offering and business rules
  - Simple on-boarding for net-ops through Windows Live Syndication Central

Microsoft Confidential

Summary – Windows Live ID

- The biggest identity provider on the planet!
- … but Live ID platform is much more than just the familiar login box
- Various types of users and various authentication models are supported
- Increasing focus on enabling federation and enterprise access to online services
- Ease-of-use is always the goal
  ….. and the challenge!

Microsoft Confidential

Bringing it all together

Microsoft Confidential

Not to be compared …

- **Open ID & OAuth** are **Standards**

  … still evolving and under development

- **Live ID** is a **SERVICE** (based on standards)
  - Identity Provider
  - Identity Federation
  - Federation Broker
  - Delegation
  - Trust Provisioning
  - Service Provisioning
  - Account Management
  - Parental Controls

  … with proven scaling for 500MM users, 1.2BN auths/day

Microsoft Confidential

But if you must compare ….

- Open ID is similar to
  - Live ID Relying Party Suite (RPS)
  - Live ID Web Authentication (WebAuth)
- OAuth is similar to
  - Live ID Delegated Auth (DelAuth)

Microsoft Confidential

Summary

- Good authentication is secure but unobtrusive
- Ease-of-use is the goal & the challenge
- Live ID Vision: Identity without borders
- Specs are “easy”, but scale is hard

Microsoft Confidential

Resources

- External: http://Dev.Live.com/LiveId
- Internal: http://LiveId
- DL: Windows Live ID Discussion (wliddisc)

Microsoft Confidential

Questions?

© 2008 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only.
Microsoft makes no warranties, express or implied, in this summary.