PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

BB22

Live Identity Services Drilldown

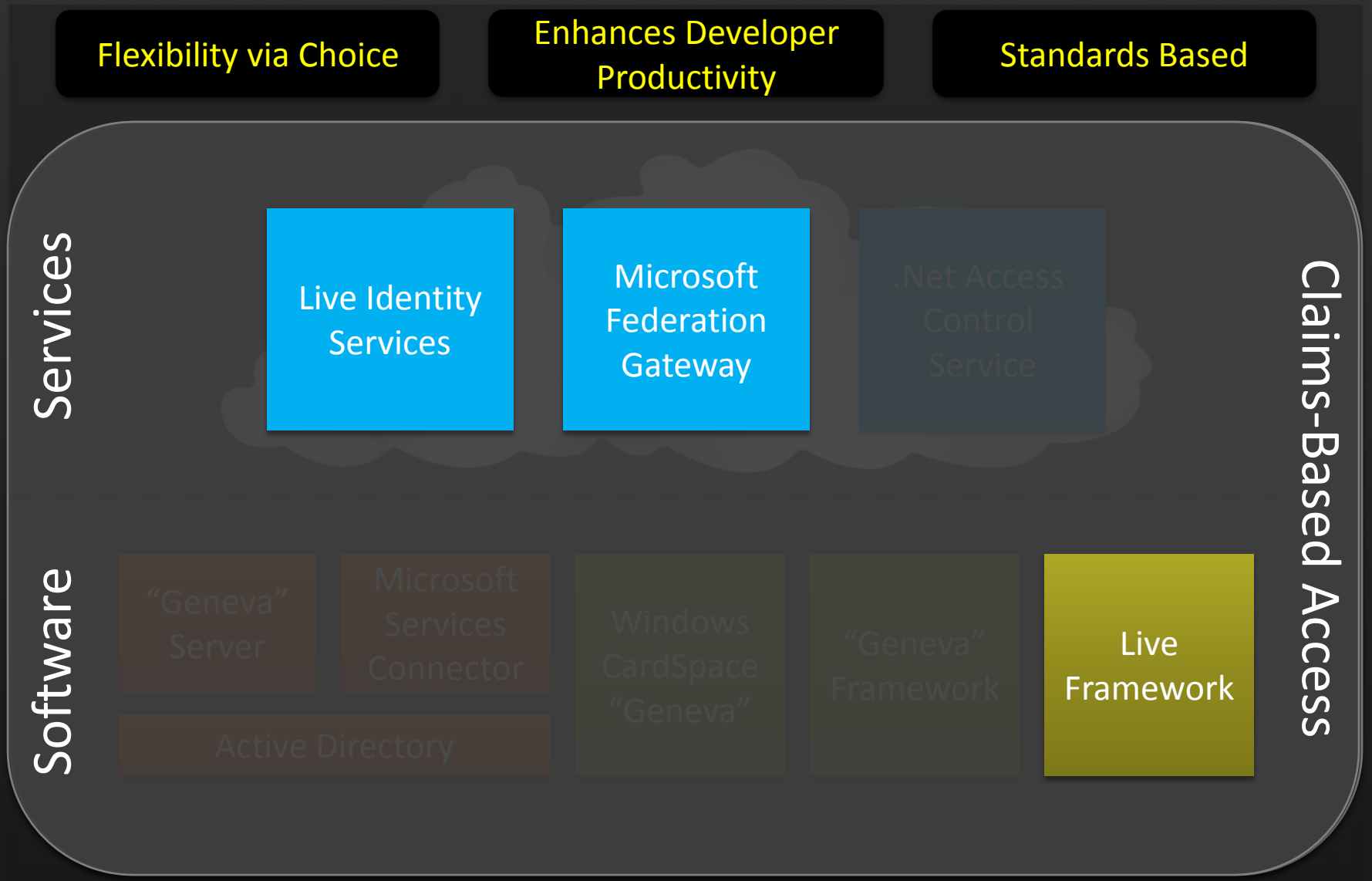
Easing the pain of identity integration

→ Jorgen Thelin
Senior PM
Microsoft Corporation

Windows Live™ ID

Microsoft Identity Software + Services

One identity model that puts users in control of their identities

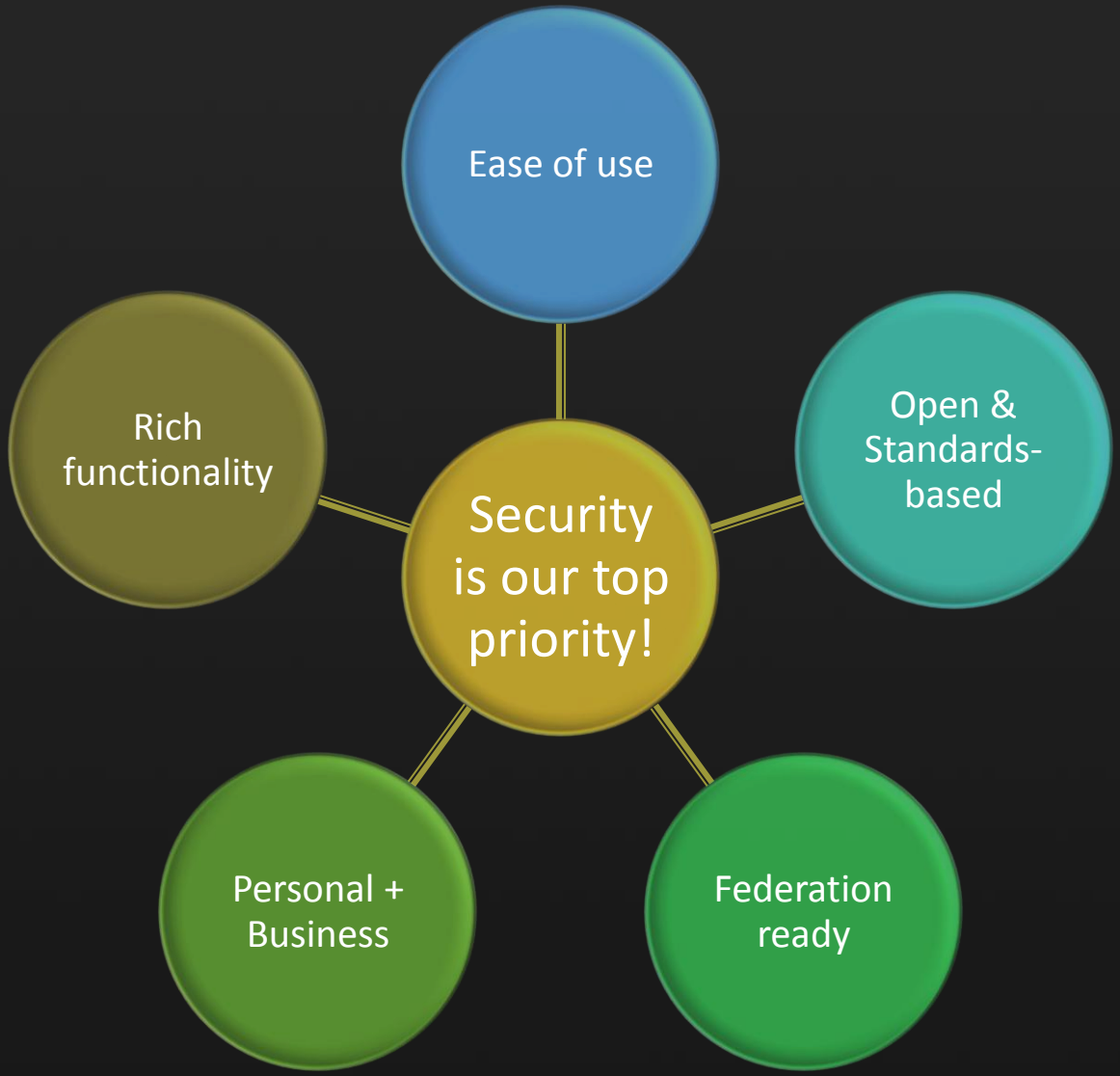


Agenda and Themes
Live Identity services

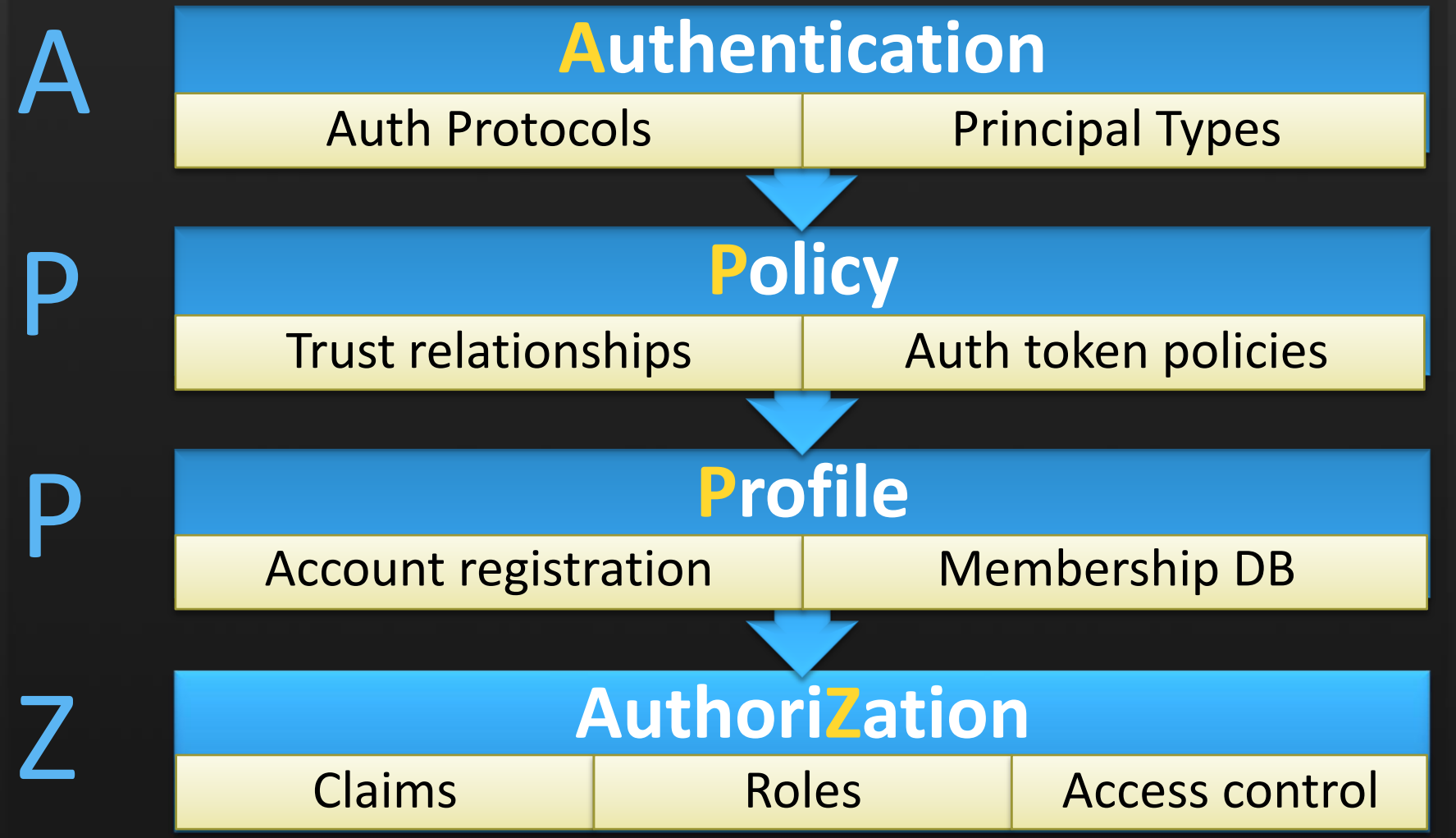
Identity Integration	• Easing the “identity pain gap”
Web Authentication	• Enabling applications to be secure
Screen Customization	• Enabling seamless sign-in/sign-up user experience
Delegated Authentication	• Enabling data portability
Rich Client Authentication	• Enabling Software + Services applications
Federated Authentication	• Enabling identity without borders
OpenID	• Embracing Open Standards

Live Identity Services

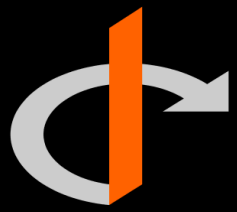
Core principles



Steps to Identity Integration - APPZ



PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE



OpenID

announcing

Windows Live ID OpenID Provider

Embracing
Open Standards

Windows Live ID OpenID Provider

Microsoft is becoming an OpenID Provider (OP)

Use your Windows Live ID account to sign-in to any OpenID 2.0 enabled Web site

What is OpenID?

- "Open ID is a free and easy way to use a single digital identity across the Internet"
  Source: OpenID Foundation - http://openid.net/
- OpenID eliminates the need for multiple usernames across different websites

Key Implementation Details

- Create **OpenID Alias** attached to your Live ID account
- Authenticate with alias + account credentials
- Choice: Either global unique (public) or pair-wise anonymous (private) identifier returned to RP

Next Steps – Try the Live ID OP

1. Set up a Live ID INT account: https://login.Live-INT.com/
2. Set up OpenID alias: **https://OpenID.Live-INT.com/beta/ManageOpenID.srf**
3. **Users**: Use OpenID 2.0 login URI: **OpenID.Live-INT.com**
4. **Library developers**: Test interop with the Live ID OP endpoint
5. **Web site owners**: Test Live ID OpenID sign-in to your site
6. Send feedback: openidfb@microsoft.com

PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

Tech Preview Demo

Windows Live ID
OpenID Provider

Embracing
Open Standards

OpenID Sign-in Request
(URL decoded for readability)

Don't panic! The SDK libraries handle all this for you!

```
GET http://openid.live-INT.com/OpenIDAuth.srf
    ?openid.mode=checkid_setup
    &openid.identity=http%3a%2f%2fopenid.live-int.com%2fjthelin
    &openid.ns=http%3a%2f%2fspecs.openid.net%2fauth%2f2.0
    &openid.claimed_id=http%3a%2f%2fopenid.live-int.com%2fjthelin
    &openid.realm=http%3a%2f%2flocalhost%3a49413%2f
    &openid.return_to=http%3a%2f%2flocalhost%3a49413%2flogin.aspx%3fRetur
    nUrl%3d%252fDefault.aspx%26token%3dAbu8voGNbjk2%252fH%252bWGN4vgbrzsE
    TS0aCY%252bCSc%252frV%252bo6kKaHR0cDovL2p0aGVsaW4ucGlwLnZlcmlzaWdubGF
    icy5jb20vDQpodHRwOi8vanRoZWxpbi5waXAudmVyaXNpZ25sYWJzLmNvbS8NCg0KaHR0
    cDovL3BpcC52ZXJpc2lnbmxhYnMuY29tL3NlcnZlcg0KMi4wDQo%253d
    &openid.assoc_handle=d7d181a0-632e-11dd-ba82-f91efcd7aef7
HTTP/1.1
```

OpenID Sign-in Response
(URL decoded for readability)

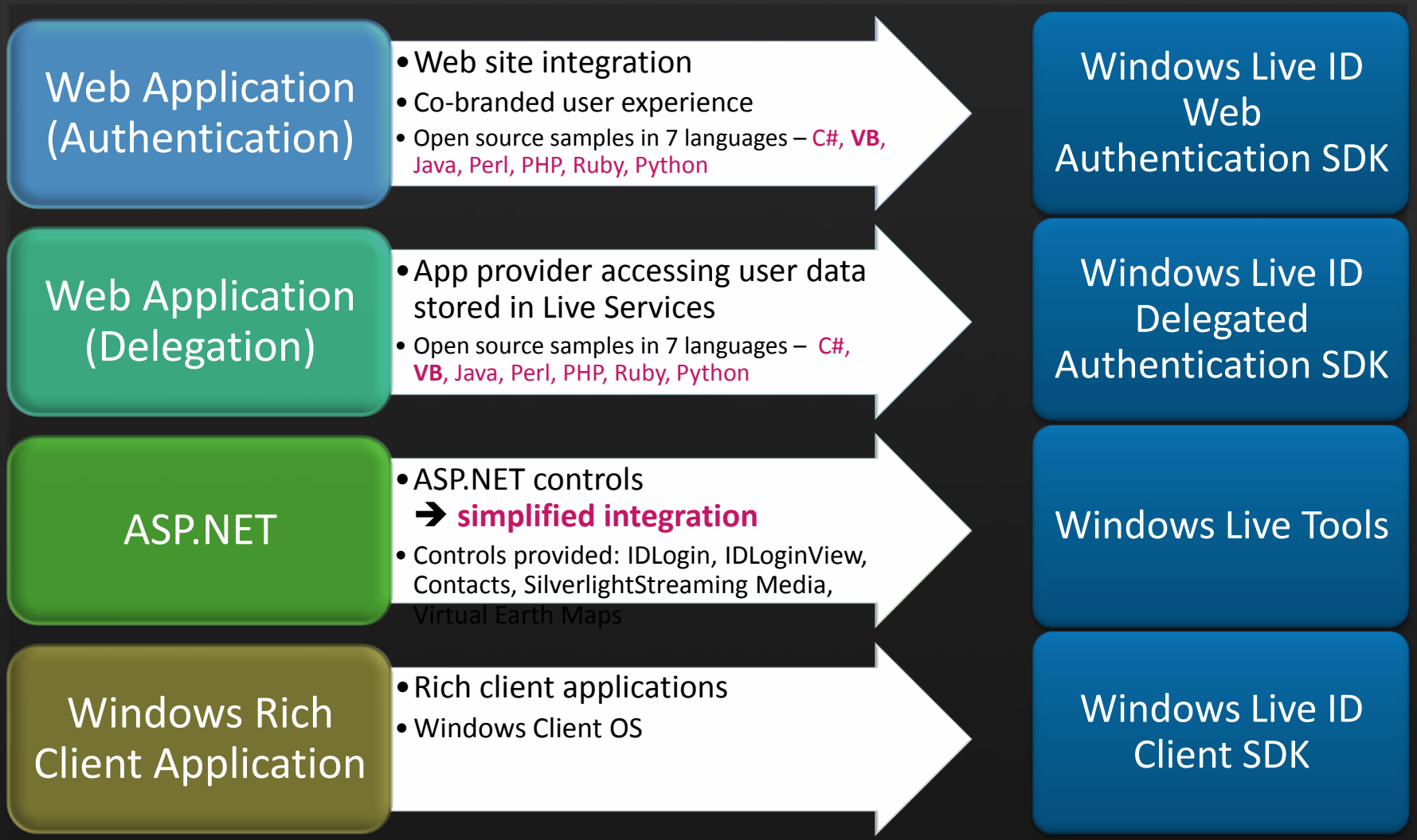
Don't panic! The SDK libraries handle all this for you!

```
GET /login.aspx
    ?ReturnUrl=/Default.aspx
    &token=Abu8voGNbjk2/H+WGN4vgbrzsETS0aCY+CSc/rV+o6kKaHR0cDovL2p0aGVsaW4ucGlwLnZl
    cmlzaWdubGFicy5jb20vDQpodHRwOi8vanRoZWxpbi5waXAudmVyaXNpZ25sYWJzLmNvbS8NCg0KaHR
    0cDovL3BpcC52ZXJpc2lnbmxhYnMuY29tL3NlcnZlcg0KMi4wDQo=
    &openid.assoc_handle=d7d181a0-632e-11dd-ba82-f91efcd7aef7
    &openid.response_nonce=2008-08-05T20:42:15ZiBs=
    &openid.ns=http://specs.openid.net/auth/2.0
    &openid.mode=id_res
    &openid.op_endpoint=http://openid.live-int.com/openidauth.srf
    &openid.claimed_id=http://openid.live-int.com/jthelin
    &openid.sig=kdXRyifqU0vd6H4kjgY5kgwmq4nN5ZhXBSck/bfLMDg=
    &openid.identity=http://openid.live-int.com/jthelin
    &openid.signed=assoc_handle,identity,response_nonce,return_to,claimed_id,op_end
    point
    &openid.return_to=http%3a%2f%2flocalhost%3a49413%2flogin.aspx%3fReturnUrl%3d%25
    2fDefault.aspx%26token%3dAbu8voGNbjk2%252fH%252bWGN4vgbrzsETS0aCY%252bCSc%252fr
    V%252bo6kKaHR0cDovL2p0aGVsaW4ucGlwLnZlcmlzaWdubGFicy5jb20vDQpodHRwOi8vanRoZWxpb
    i5waXAudmVyaXNpZ25sYWJzLmNvbS8NCg0KaHR0cDovL3BpcC52ZXJpc2lnbmxhYnMuY29tL3NlcnZl
    cg0KMi4wDQo%253d
HTTP/1.1
```

PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

Integrating with Live Identity Services

Live Identity Services
Integration SDKs



Live Identity Services
Type of identity

Principal Types

Principal	Acting for Self	Acting for User
User	User auth (Client or Web)	
Application	App auth (AppID)	Delegation (Good) Impersonation (BAD!)
Device	DeviceID	Linked DeviceID

Credential Types

- [Strong] Password, Pin
- eID / Smart card
- CardSpace
- Policy-driven control

The Password Anti-Pattern!

Types of Live ID Users

- Live Mail / Hotmail accounts
- EASI (“E-mail As Sign-In”)
- Managed domains
- Federated domains

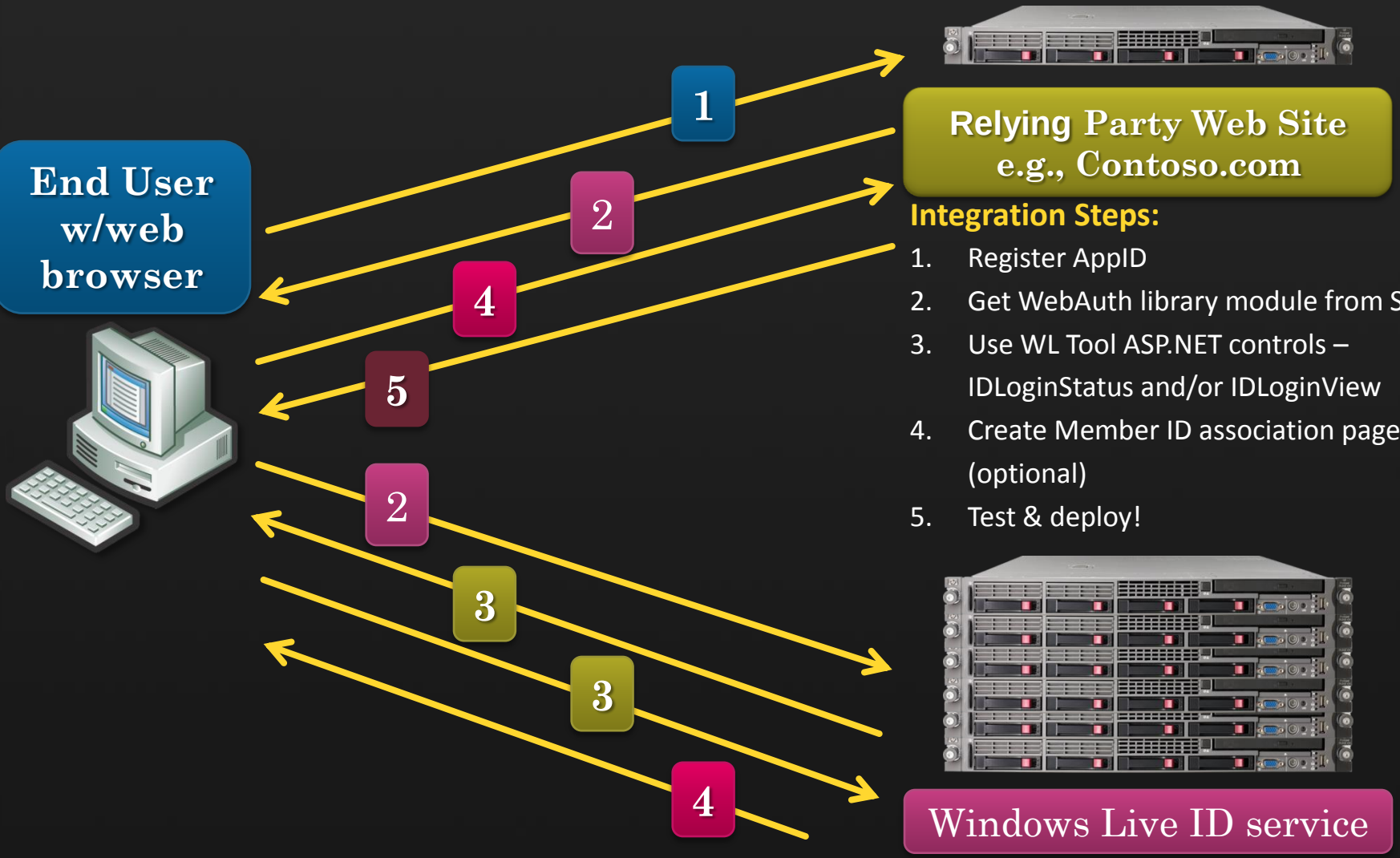
demo

Live Identity Services Web Authentication

Enabling apps
to be secure

Web Authentication Protocol Overview

Windows Live ID Web Authentication SDK Docs http://go.microsoft.com/fwlink/?LinkID=91762



Integration Steps:

1. Register AppID
2. Get WebAuth library module from SDK
3. Use WL Tool ASP.NET controls – IDLoginStatus and/or IDLoginView
4. Create Member ID association page (optional)
5. Test & deploy!

Windows Live Tools
IDLoginStatus Control (ASP.NET)

```
<live:IDLoginStatus
  ID="IDLoginStatus1"
  runat="server"
  ApplicationContext="welcomepage"
  BackColor="#E5ECE5“
  onserversignin=
    "IDLoginStatus1_ServerSignIn"
  onserversignout=
    "IDLoginStatus1_ServerSignOut"
/>
```

WebAuth Sign-in Control
(Cross-platform HTML – URL decoded for readability)

```
<iframe id="WebAuthControl"
  src="http://login.live.com/controls/WebAuth.htm
    ?appid=<%=AppId%>
    &context=welcomepage
    &style=font-size=10pt;
      +font-family=verdana;
      +font-style=normal;
      +font-weight=bold;
      +background=white;
      +color=black;"
    width="80px" height="20px">
</iframe>
```

WebAuth Sign-in Messages

Don’t panic! The SDK libraries handle all this for you!

Sign-in Request

- GET
  http://login.live.com/wlogin.srf
  ?appid=00167FFE80002700
  &appctx=welcomepage
  HTTP/1.1
  ...

Sign-in Response

- POST http://www.mydomain.com/wl-handler.aspx HTTP/1.1

  action=login
  &appctx=welcomepage
  &stoken=MA12BCF0012BAM567890MABD123456ABCDEF12345667890

Encrypted Contents:
appid=<application id>
&uid=<user identifier>
&ts=<timestamp>
&sig=<signature>

PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

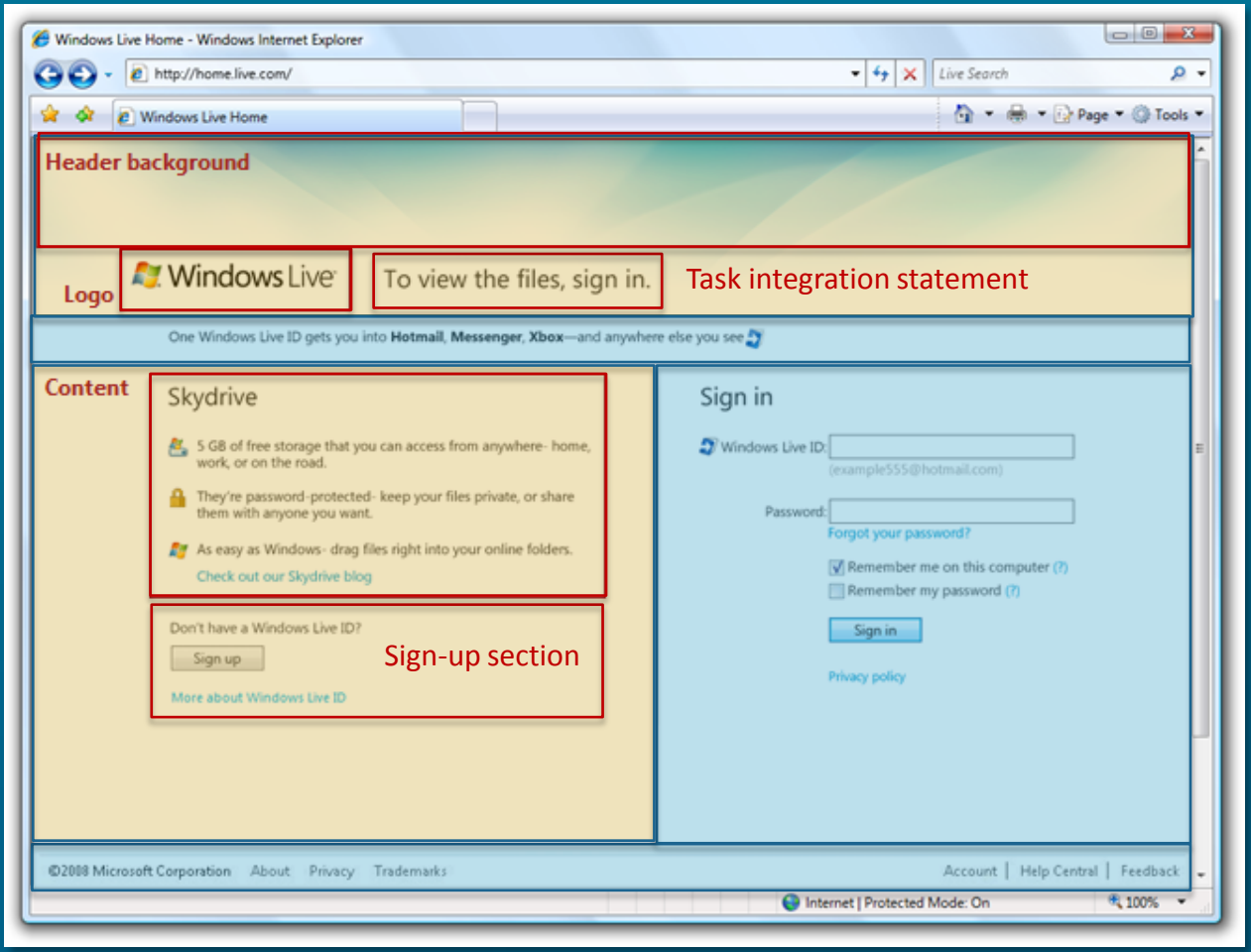
Tech Preview Demo

Live Identity Services Web Authentication with Sign-in Screen Customization

Enabling seamless sign-in / sign-up user experience

Customizable Sign-in Screen

- Flexible sign-in customization options allow creative and seamless user experience



Customizable Contents Area (Orange)

Elements that can be customized.

- Partner Logo
- Task statement
- Product description
- Sign up section
- Header background

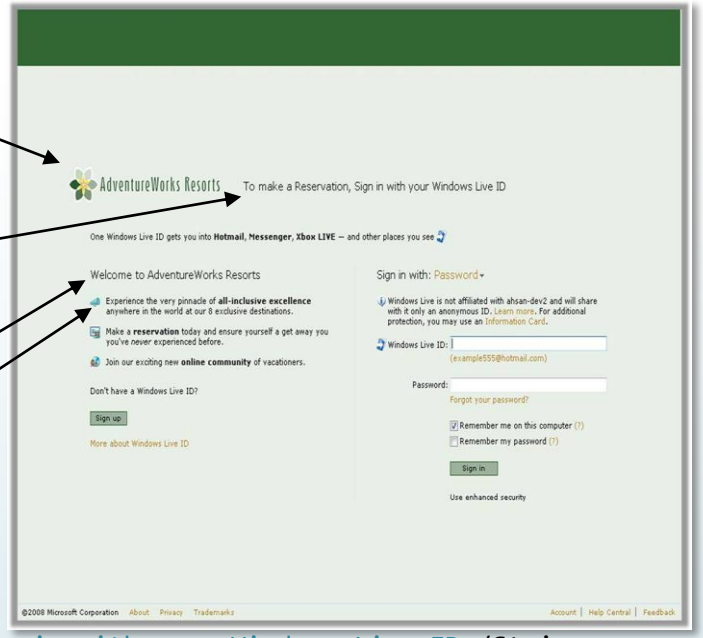
Customizable Theme Area (Blue)

Elements cannot change. Customize look & feel.

- Font color
- Background color
- Button color
- User tile color
- Live ID description color

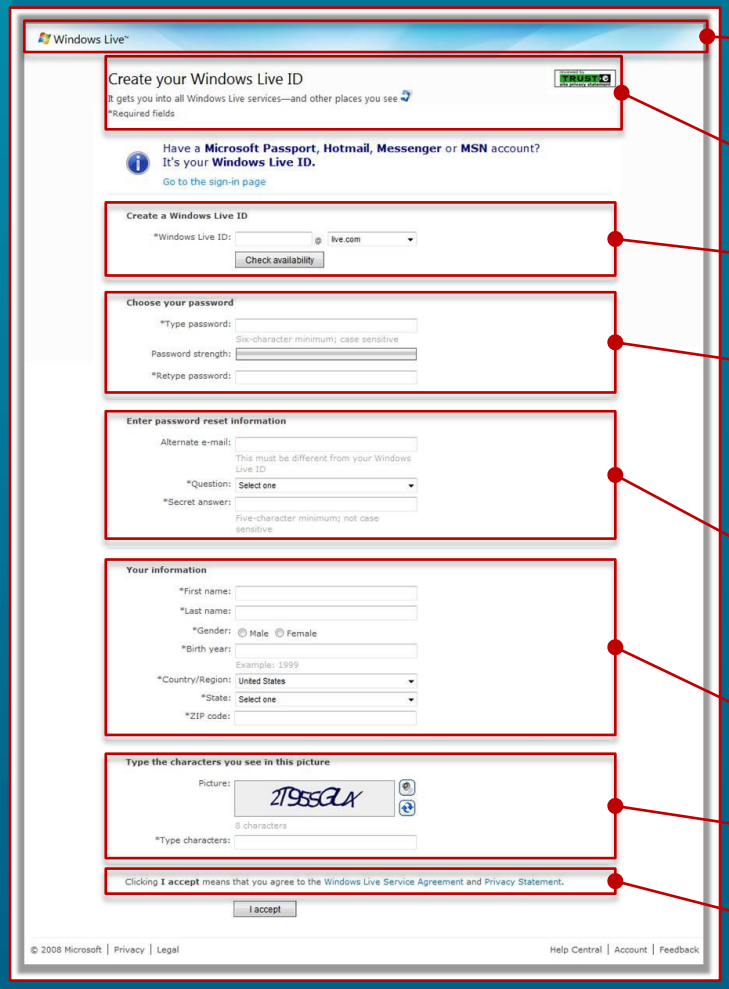
Sign-in Screen Customization XML

```
<WhiteLabelProperties>
      <Logo>STRID_LOGO</Logo>
      <LogoAltText>STRID_LOGOALTTEXT</LogoAltText>
      <HeaderBkgndColor>#336633</HeaderBkgndColor>
      <BkgndColor>#e5ece5</BkgndColor>
      <FontColorLight>#b5781e</FontColorLight>
      <FontColorLink>#b5781e</FontColorLink>
      <ButtonColor>#9EB39B</ButtonColor>
      <ButtonBorder>#336633</ButtonBorder>
      <FontColor>black</FontColor>
      <UserTileColor>#C6D6B9</UserTileColor>
</WhiteLabelProperties>
<SiteLoginUIProperties>
      <Header id ="default">STRID_HEADER</Header>
      <Title id="default">STRID_TITLE</Title>
      <Subtitle id="default">STRID_SUBTITLE</Subtitle>
</SiteLoginUIProperties>
<StringTable>
      <Language langID="en">
            <String id="STRID_HEADER">To make a Reservation, Sign in with your Windows Live ID</String>
            <String id="STRID_TITLE">Welcome to AdventureWorks Resorts</String>
            <String id="STRID_SUBTITLE">
            ##li5## Experience the very pinnacle of ##b##all-inclusive excellence##/b##
                  anywhere in the world at our 8 exclusive destinations.
            ##li2## Make a ##b##reservation##/b## today and ensure yourself
                  a get away like you've ##i##never##/i## experienced before.
            ##li3## Join our exciting new ##b##online community##/b## of vacationers.
            </String>
            <String id="STRID_LOGOALTTEXT">AdventureWorks Resort</String>
            <String id="STRID_LOGO">
            http://adventureworksresorts.sharplogic.com/App_Themes/AWR/images/logo.png
            </String>
      </Language>
</StringTable>
```



Customizable Registration Screens

- Flexible registration screen options



Header image

Task integration

Username

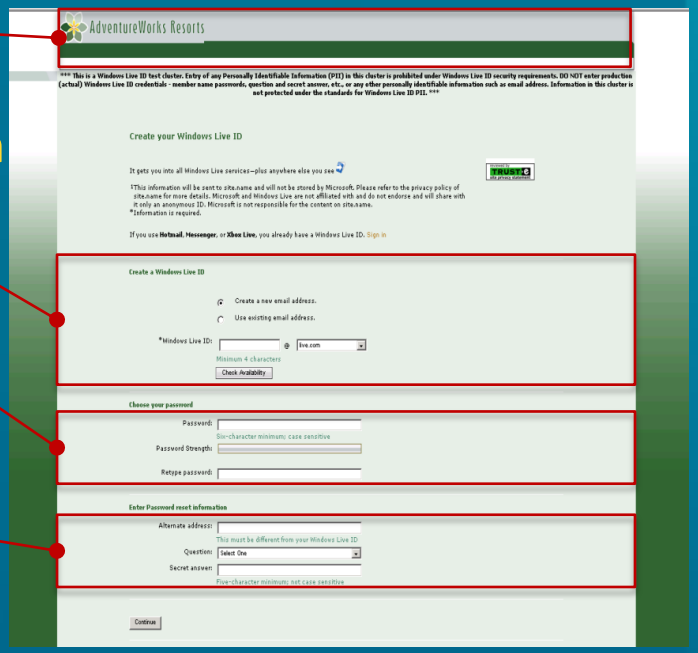
Password

Password reset question / Alt e-mail

Profile info

CAPTCHA

ToS



PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

Live Identity Services Delegated Authentication

Enabling data portability

Delegated Auth Protocol Overview

Windows Live ID Delegated Authentication SDK Docs http://go.microsoft.com/fwlink/?LinkID=107420

End User w/ browser

Integration Steps:

1. Register AppID
2. Get DelAuth library module from SDK
3. Create consent request URL link
4. Create auth callback handler page
5. Create store for consent tokens (optional)
6. Send RP data request and process reply
7. Test & deploy!

Application Provider (web site)

"Granting Consent" phase (user 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

Requesting Delegated Auth Consent

Don’t panic! The SDK libraries handle all this for you!

```
https://consent.live.com/delegation.aspx
    ?ru=http://mydomain.myapp.com/ReturnURL.aspx
    &ps=Contacts.View,Contacts.Update
    &pl=http://mydomain.myapp.com/PrivacyPolicy.htm
    &ttype=1
    &mkt=en-US
    &app=appid%3d10000%26ts%3d1193445084%26ip%3d157.56.1
    90.178%26sig%3d7HgcsIEheEVO30BuPAEJhJeB8Pz0xHBV%252f%2
    52bQD27AOdmI%253d
    &appctx=welcomepage
```

1=Compact token, 2=SAML token

Application Verifier token:
AppID, Timestamp, Client IP, SHA256 signature

DelAuth Consent Token Response (URL Decoded)

Don’t panic! The SDK libraries handle all this for you!

delt=EwCoARAnAAAUgxwUrFTrj0j98kTTv4OX%2FOkhSc2AADHt9dXtiWa4afIM
1AtKBgDzW2LOYBmExjIAumf%2B33MyPpGSnwrmtOc2aKG0Oz008Jg6a9Ss8a6L4
zi8Za9gT85eqqdS0HNJZW9xAUoD2MOqUz7RxqY%2FpNhAWm6ndhFTj9VWWZYi7z
IJJU7RgrIXEJrmQsHSKN1%2B2Iot56mknEECA2YAAAi5VYs8bPiGofgAEiVBGu8
ve8kv459FJn8ioXFJMR4f5EYNJqxMXG8tZhe87ylkvESebImX%2B4T8EGxxgDBT
THmEnK5PtoxJDTLJCSz4UJwRPAS0KW2H5TIi7Ecu6dZ5FbspeKlPCi7pxjevW1W
AHuoJY9oow%2FgUCZhcxCusUg2Cg6LmpSm0KwacVzaXLEOwwpfUXtFSwpPsU8w8
G9syt4%2F0k1W4HJmdrqU1xqHO7ZEX3JBWpKBscNbKr5z3qCkO2tpW%2BBjFEgy
8w%2Fc5wb66At7V4Vs1ccbiBJ7pC%2F0VjyfzKfBYNP2zniAmepap2jY780q73C
zc10w0bfMr54cKMaDrK6kAAA%3D%3D

&exp=1196836447

&reft=F7BJdi2ojtPWXv7qVCKrhD0kU35Rf1k4wz0nFxgB33czSkOgk0Ht5n8LGLZW2Mgo
06dpFYonRF0e0hasWS91l37cf8sq2NaxyXJASrEdKoYOApPUBI6RqYnDSBgkNqKPQtUbIN%2
F%2FXQ%2B7qUnzyWvnSA%3D%3D

&offer=Contacts.View,Contacts.Update:1228350847

&sig=C1itgV6AL7%2F%2BJFnML1unjGZ6nNNjQsrb8%2BcTtmNAzp8%3D

&skey=iS30MXEnIJj7K6HpwUBrXR5isE9rN9zq

&lid=f8eb4468555a951e

PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

Live Identity Services Federated Authentication

Enabling identity without borders

Federated Authentication Overview

- Federation is the glue that enables an open identity system
  - Interop with other Identity Providers via agreed protocols
  - Based on existing WS-* standards - WS-Federation / WS–Trust / SAML
- Federation requires unidirectional or bidirectional trust relationship(s) between organizations
  - Federation involves three parties:
    - **Identity Provider** (IdP) authenticates users' identity accounts
    - **Relying Party** or Resource Provider (RP) permits access to resources in their network
    - **Federation Provider** or Gateway brokers access between Federated Identity Providers and Relying Parties
  - Result: Authentication assertions from one organization recognized by the other

Federated Authentication Flow

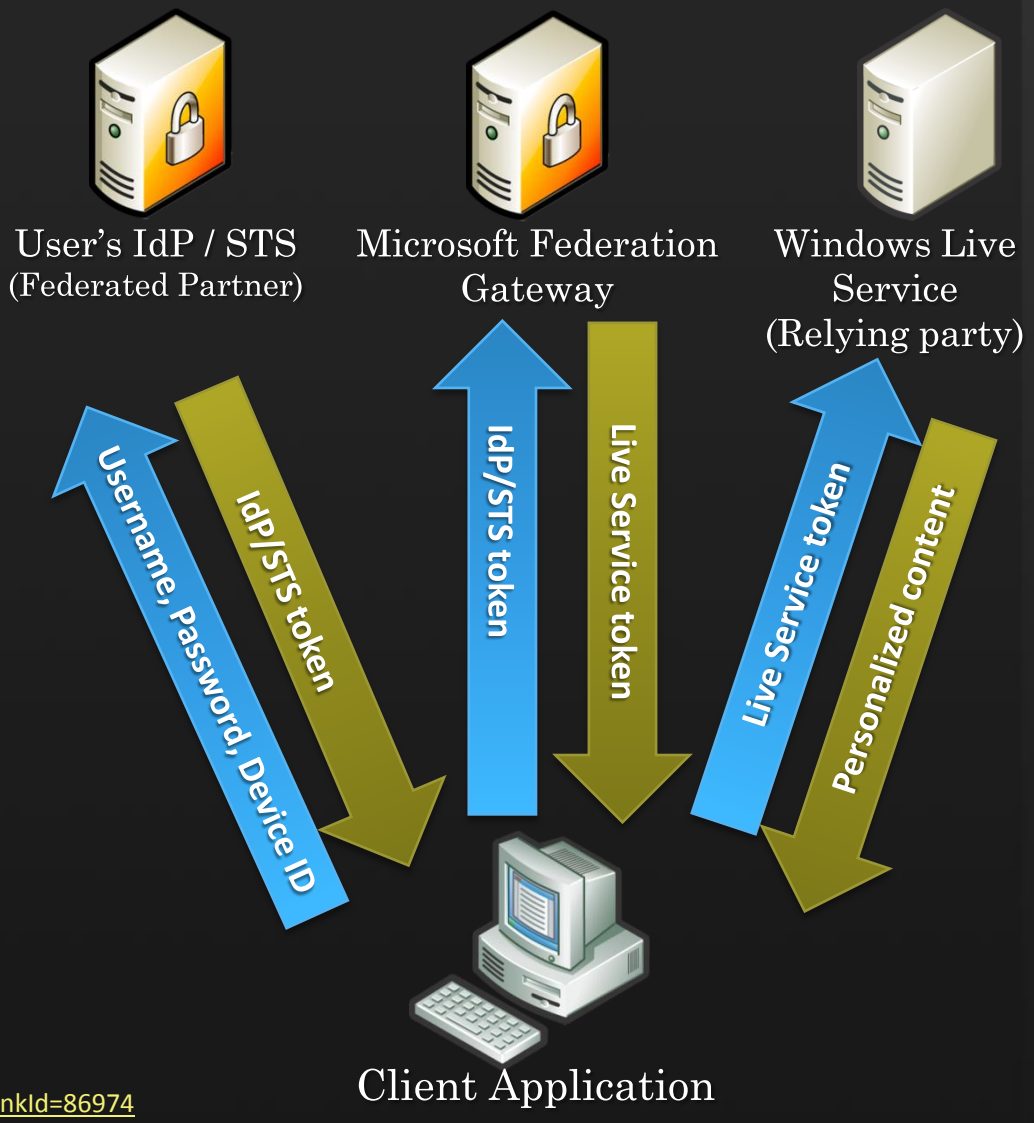
Step 1 (Partner Sign-in)
A user sends credentials to the federated partner identity provider (IdP).

federated partner's *Security Token Service (STS)* generates IdP token.

Step 2 (Federated Sign-in)
IdP token is sent to Microsoft Federation Gateway.

Federation Gateway converts IdP token from the federated partner to a Live Service token.

Step 3 (Service Sign-in)
The issued service access token is sent to the Live Service that the user originally wanted to access.



Windows Live ID Client SDK http://go.microsoft.com/fwlink/?LinkId=86974

Summary
Live Identity Services

Identity Integration	• Easing the “identity pain gap”
Web Authentication	• Enabling applications to be secure
Screen Customization	• Enabling seamless sign-in/sign-up user experience
Delegated Authentication	• Enabling data portability
Client Authentication	• Enabling Software + Services applications
Federated Authentication	• Enabling identity without borders
OpenID Support	• Embracing Open Standards

Core Principles

- Ease of use
- Rich functionality
- Open and Standards-based
- Personal + Business
- Federation-friendly
- Security is our top priority!

Easy

Into the Future

- More ease of use – for users and developers
- More standards
- More open integration
- Never let up on security!

PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

Q&A

Please use the microphones provided

Live Identity Services
Resources and links

- Windows Live ID Developer Center - http://dev.live.com/liveid
  - Windows Live ID Articles on MSDN - http://go.microsoft.com/fwlink/?LinkId=111111
  - Windows Live ID Documentation on MSDN - http://msdn2.microsoft.com/en-us/library/bb404787.aspx
  - Windows Live ID Developer Forum - http://go.microsoft.com/fwlink/?LinkID=78146
  - Windows Live ID Team Blog - http://winliveid.spaces.live.com
- Windows Live ID Whitepapers
  - Introduction to Windows Live ID - http://msdn2.microsoft.com/en-us/library/bb288408.aspx
  - Understanding Windows Live Delegated Authentication - http://msdn2.microsoft.com/en-us/library/cc287613.aspx
  - Windows Live ID Federation - http://msdn2.microsoft.com/en-us/library/cc287610.aspx
- Windows Live ID Documentation and SDKs
  - Windows Live ID Web Authentication SDK Docs http://go.microsoft.com/fwlink/?LinkID=91762
    Web Authentication SDK Samples http://go.microsoft.com/fwlink/?LinkID=91761
  - Windows Live ID Delegated Authentication SDK Docs
    http://go.microsoft.com/fwlink/?LinkID=107420
    Delegated Authentication SDK Samples http://go.microsoft.com/fwlink/?LinkId=107419
  - Windows Live ID Client SDK download - http://go.microsoft.com/fwlink/?LinkId=86974
- Delegated Authentication Resource Providers List - http://go.microsoft.com/fwlink/?LinkID=108535
- Windows Live ID Web Authentication app registration page http://lx.azure.microsoft.com
- Windows Live Tools for Visual Studio - http://dev.live.com/tools/

Related Sessions

- BB11 – Identity Roadmap for Software + Services
  - The security demands on applications continue to grow in the face of compliance, online threats, and cloud- based software. In this session find out how to use Microsoft's portfolio of identity software and services to advantage your connected applications. Learn about the future roadmap for Identity and the claims-based architecture underlying it all, from Windows Live ID to Active Directory, from on-premises software to the cloud, and anchored in industry standard protocols.

- BB29 – Identity: Connecting Active Directory to Microsoft Services
  - Learn how to augment your existing IT infrastructure with Microsoft Services. Manage and secure end-user access to cloud services using your existing investment in Active Directory. Enable end users to access Microsoft services through existing Active Directory accounts, the same way they access your intranet-hosted software today. Hear how to enable existing software to use new service capabilities without re-writes, and do it all through the use of open and standard protocols.

Evals & Recordings

PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE

Microsoft®

Your potential. Our passion.™


Microsoft
PDC2008
PROFESSIONAL DEVELOPERS CONFERENCE