

# Identity Workshop:

- The Value
- The Technology
- The Future

Eric Sachs

Senior Product Manager, Google Security

# My Identity

## Enterprise Space

2008 - Cloud Computing (Google Security, Google CIO)

2003 - SaaS (Google Apps for your Domain)

1997 - ASP (co-development with both IBM/Lotus and Microsoft)

1992 - Email Outsourcing (Lotus Notes/cc:Mail)

## Consumer Space

Google Accounts, Google Health, orkut.com, ...

## Internet Standards

OAuth, OpenID, WRAP, OpenSocial, ...

# Slides online

- Slides available in case your IT admin wants to know more
- Google search for "oauth goog" and click first result
  - Or <http://bit.ly/esachs>
- Search on the page for Cloud Identity Summit

# Identity: The Future

- We showed a higher value proposition
  - as Chris Messina covered
- We overcame a bad usability reputation
  - Usability Summits, Hybrid Onboarding success rate, ...
- We overcame security concerns
  - Government adoption, OIX, Enterprise adoption
- We matured an industry organization
  - Executive director, more sponsors, more awareness

...but there is still homework we know needs to be done

# Functionality from major Email IDPs

	gmail.com	hotmail.com	yahoo.com	aol.com
Simple consent page	YES	YES	YES	YES
Email Address	YES	YES	YES	NO
Avoid reprompt on return visit	YES	YES	NO	NO
Address Book API	YES	YES	YES	NO
Standards based	YES	NO	YES	YES



## Connect ISDK to Messenger

Communicate with your Windows Live Messenger world on **isdk.dev.live.com** or share information like your profile, photos, or friends.

[What will I share?](#)

eric.sachs@gmail.com

[Sign in with a different account](#)

Connect automatically



[Sign in as a different user](#)

**Plaxo.com** **Google**

**Plaxo.com** is asking for some information from your Google Account **rgbsbc@gmail.com**

- Email address: Greg and Barb Sachs (rgbsbc@gmail.com)
- Language:English
- Google Contacts

Remember this approval


You can always change your Google Account approval settings. Plaxo.com is not owned, operated, or controlled by Google or its owners. [Learn more](#)

Yahoo! Review and Continue - Google Chrome  
https://open.login.yahoo.com/openid/op/start?z=oliqdwZR.ZIFUjqlF-4iCuU6.iPCGwf8MnUZaAvBu

**YAHOO!** Hi, Eric | Sign Out | Help

Click "Agree" to sign in to signin.myscars.com using your Yahoo! ID and allow sharing of Yahoo! info.

You are sharing the following:

 **Eric Sachs (Eric)**  
Male - initfounder@yahoo.com  
Language: English

**Agree**

By clicking Agree you are agreeing to the [Yahoo! Additional Terms of Service](#) AND to the [signin.myscars.com's policy](#).

Copyright © 2010 Yahoo! Inc. All rights reserved.  
[Copyright/IP Policy](#) | [Terms of Service](#) | [Guide to Online Security](#) | [Privacy Policy](#)

https://profileservice.aol.com/getConsent.jsp?enc=/wQBAAAA...  
https://profileservice.aol.com/getConsent.jsp?enc=/wQBAAAAADHZ0nTCWvvvM6QO9LphMD%2Bc

**AOL**

### Request for Information About You

<https://signin.myscars.com/>

is requesting that AOL send it the information below. You are not required to provide the website with any of this information and can choose which data you send to the website by checking the box next to each line of information. You can also edit the Information before AOL sends it to the website.

AOL has no control over any of the information once it is sent to the website and is not responsible for how the website uses the information. In addition, AOL cannot modify or retrieve any information once it is sent to the website. You should read the privacy policy of the website located [here](#) prior to sending the information.

Additionally, AOL will store any updates you make to the Information for your future use of AOL products and services.

Nick Name

Birthday

Home E-mail

Language

Time Zone

Gender

Zip Code

Country

By clicking the checkbox next to any line of information above and the "Send" button below, you are granting AOL permission to send that information to the website and for AOL to store the updated information for future use of AOL products and services and sites supporting OpenID. Click the "Do Not Send" button below if you want to stop and not send any information to the website.

# Reduce Technical delta

- Functional consistency makes business owners happy
- Engineers dislike the lack of technical consistency
  - SAML, OpenID, AX, SREG, Facebook Connect, BBAuth, AuthSub, OAuth, OAuth-WRAP, OAuth2, ...
- Increased usage has turned-up edge-cases that technology needs to address
  - Mobile usage
  - Installed applications
  - Complexity of crypto
  - Mapping to existing government security publications
  - IDP and RP SaaS vendors
  - Certification
  - ...



# Future of OAuth



- OAuth 1
  - Original goal - reduce technical delta between highly overlapping schemes from Yahoo, Google, MSFT, AOL, etc.
  - Reality - we over designed it and developers found it too difficult
- Unexpected Enterprise interest
  - [Results](#) of Microsoft Azure technical preview - "REST web services are clearly increasing in popularity with both Web and enterprise developers. What is also apparent is a significant gap has emerged in the market place for REST-based identity and access control technologies."
  - How does your recruiting system prove its identity when accessing the APIs of your HR system?

# Web-service security

Consistent Enterprise feedback to cloud vendors like Microsoft & Google:

1. A new technique is needed for web-service authentication in the cloud. ("Role accounts" on internal IPs are not sufficient)
2. The technique needs to work with REST APIs
3. Enterprise developers should not have to worry about crypto
4. The technique needs to be an open industry standard, both to avoid lockin, and to get a detailed review by the security community

# OAuth WRAP Profile

- Nov 2009: Announced by Microsoft, Google, & Yahoo
  - <http://www.google.com/group/oauth-wrap-wg>
  - Leverages design patterns from Kerberos, WS-Trust, and Yahoo's scalable OAuth extension
- Nov 2009: [Azure AppFabric support](#)
- May 2010: [Google experimental support](#)
- June 2010: [MS Live ID API support](#)

# OAuth 2.0

- OAuth 1 + OAuth-WRAP + IETF = OAuth 2.0
- Expanded participation with other major vendors such as Facebook, Salesforce, Twitter, etc.
- Goal to finalize spec in 1-2 months
- Implementation of draft spec by companies such as [Facebook](#)
- Biggest differences from OAuth 1:
  - More profiles for methods to get a token
  - API providers must have an SSL endpoint
  - Tokens can be used for API calls without additional crypto

# Future of OpenID

- OpenID
  - Original goal: URL as ID
  - Reality: Email as user-visible ID, URL as hidden ID
- Unexpected Problems
  - Mobile usage - especially browser URL length
  - Installed applications
  - US government's historical LOA (level-of-assurance) guidelines
  - IDP and RP SaaS vendors
  - Certification
  - ...

# Possible Paths

1. OpenID V2 extensions
  - But extensions make URL length problems worse
2. OpenID v.Next
  - A list of goals, but not a technical proposal
3. Artifact Binding
  - Strong framework, but big technical changes
4. OpenID on OAuth2
  - Also a big technical change, but on a framework providers were already using
  - Mapped well to existing Artifact Binding design
  - Supports installed-apps
  - Provides an option for "simple" identity providers

# OpenID on OAuth2

Simple IDPs: Timeframe for identity on OAuth2=now

- Optimize for an RP that only trusts one IDP
- No discovery, no validation of assertion, simpler UI
- Examples:
  - Twitter
  - Microsoft Live
  - LinkedIn
  - FourSquare
  - Facebook

Complex IDPs: Timeframe for OpenID+OAuth2=Q4?

- Add back in UI challenges, discovery, validation of assertion, certification, ...

# Moving from IDPs to RPs

- Future for IDPs:
  - Functional consistency, Technical consistency, OAuth2, ...
- What about RPs?
  - Lots of websites with Facebook, Google, Yahoo buttons..
  - But how many large websites have those login buttons?
  - And how many of those websites already had a login system with lots of user accounts?



# Short advice

- If you have a large installed base of registered users you care about, you absolutely should wait till the end of the year
- If you are willing to take the risk of hurting your existing registered users, but want a lot more registered users, then use vendors like RPX/FriendConnect that hide the variance in plumbing
- The middle of the road options is to pick a single identity provider (Facebook or Google for consumers, GoogleApps for enterprises) but it is dangerous in both cases because best practices are not yet known

# Example problems

- Sam calls customer service to complain that even though he only uses one email address for his personal stuff, he has two accounts at your website. How did that happen?
- sam@yahoo.com has an existing account with a password, how does your site link it to an identity provider?
- sara@acme.com is fired, but still controls an account with that Email on MSFT Live, Facebook, Google, etc. How do you know not to trust the accounts from those identity providers?
- ...

# Example problems

- Your site's iPhone/Android app asks users for their password, but how do users without a password login to the app?
- Tom changes his Google Account email from his old school address to his new @gmail.com address. How should that impact his account on your site?
- Jack's email provider offers multi-factor authentication. Can he still use his Twitter account with the same email to login with just a password?
- ...

For more details

- Google search for "oauth goog" and click first result
  - Or <http://bit.ly/esachs>
- Search on the page for "account-linking"

# What are the best practices?

- The identity community as a whole has been working to research, test, and document best practices.
- What Google is doing
  - Launched an IDP for Google Accounts and gathering some feedback
  - Launched Google Apps Marketplace for 2+ million domains, and gathering even more detailed feedback
  - Launching a new RP user-interface for our SAML enabled enterprise customers
  - Attempting to launch an RP to yahoo.com, hotmail.com, and aol.com to provide a large example site that others could mimic

**Marketplaces**

**Google Apps**

Products

- Accounting & Finance
- Admin Tools
- Calendar & Scheduling
- Customer Management
- Document Management
- Productivity
- Project Management
- Sales & Marketing
- Security & Compliance
- Workflow

Professional Services

- Archiving & Discovery Implementation
- Custom Application Development
- Google Analytics
- Medium-Large Business Implementation
- Small Business Implementation
- Support & Managed Services
- Training & Change Management

**Enterprise Search**

Products

- Content Connectors
- OneBox Modules
- Search Extensions

Professional Services


- GSA Deployment
- Google Mini Deployment
- Custom Development
- Training
- Co-Spatial Solutions

The Google Apps Marketplace offers products and services designed for Google users, including installable apps that integrate directly with Google Apps. Installable apps are easy to use because they include single sign-on, Google's universal navigation, and some even include features that integrate with your domain's data.

### Featured Apps

**SurveyMonkey**

Now you can access the world's most popular web-based survey solution through your Google Apps environment. Quickly and easily gather the insights you need to move your business forward.



• **Try popular & notable apps**



**Dito Directory - Shared Contacts Manager**

Dito Directory is a contact manager that gives domain administrators the power to upload, create, and modify Domain Shared Contacts and User Profiles that are shared across the domain.



**Zoho CRM (3 users free)**

Zoho CRM offers businesses a complete customer relationship life-cycle management solution for managing organization-wide Sales, Marketing, Customer Support & Service and Inventory Management.



**Solve360 :: CRM Meets Project Management for Serious Business**

Solve360 is a modern collaborative CRM service that integrates features to manage client projects. It's ideal for small teams that

**"Tops" in Google Apps**

Top rated

1. [RunMyProcess - Workflows and Integration for Google Apps](#)  
★★★★★ 39 reviews
2. [OffiSync - \[FREE\] Integrate Microsoft Office with Google Apps](#)  
★★★★★ 224 reviews
3. [\[FREE TRIAL\] Syncplicity Business Edition](#)  
★★★★★ 37 reviews
4. [Smartsheet Project Management for Google Apps](#)  
★★★★★ 54 reviews
5. [Socialwok: Free Business Social Productivity & Customer Management](#)  
★★★★★ 57 reviews

Top installed

1. [Manymoon: Free Social Productivity, Project Management & Task Management](#)  
★★★★★ 94 reviews
2. [Aviary Design Suite \(Free\)](#)  
★★★★★ 11 reviews
3. [OffiSync - \[FREE\] Integrate Microsoft Office with Google Apps](#)  
★★★★★ 224 reviews
4. [Zoho CRM \(3 users free\)](#)  
★★★★★ 21 reviews
5. [TriplIt - Free Travel Organizer](#)  
★★★★★ 8 reviews

# All your travel plans in one spot.

Just forward your travel confirmation emails to [plans@tripit.com](mailto:plans@tripit.com).

## Build your itinerary

Email TripIt your travel plans—airline, hotel and more—it doesn't matter where you book.

## Get Organized

TripIt organizes your plans in a master travel itinerary that's easy to share and access.

## Stay informed

Automatically monitor your TripIt itineraries and get alerts about any travel delays with TripIt Pro.

## Sign up for TripIt



Send me TripIt updates and tips

**Sign up - it's free!**

Or, sign up with...


 Google  Google Apps

 Facebook

By clicking Sign Up, you confirm that you accept the [User Agreement](#). We don't share your email address. [More info](#)



 "Easy-to-edit itinerary"  
Frugal Traveler, NY Times

 "Everything is organized in one place... you'll be totally prepared."  
Time.com 50 Best Websites 2009

 "A simple travel service that is absolutely awesome."  
TechCrunch



# Track Your Email within Zoho CRM Now!



- Track Leads & Contacts
- Communicate using e-mails
- Share your e-mails with colleagues
- Build better customer relations

**Get Started**

Sign in using Google Apps Account



WWW.

Go

eg: yourdomain.com

« [Back to Sign In](#)

**AlertBlue**

[Sign in as a different user](#)

**Accounts.zoho.com** is asking for some information from your AlertBlue account **admin@alertblue.com**

- Email address: AlertBlue Admin (admin@alertblue.com)
- Language: English

**Allow**

**No thanks**

Remember this approval

You can always change your AlertBlue account approval settings. Accounts.zoho.com is not owned, operated, or controlled by AlertBlue or its owners. [Learn more](#)

# Google as a SAML RP

- Google Apps Premier
- SAML enabled domains
- Google has no password for these users
- What does user type in Google's login box?
- Training user to login w/o password



Google Accounts


https://www.google.com/accounts/ServiceLogin?passive=1209€


# Google accounts


**Sign in to personalize your Google experience.**


Google has more to offer when you sign in to your Google Account. You can customize pages, view recommendations, and get more relevant search results.

Sign in on the right or [create one for free](#) using just an email address and password you choose.

 [Gmail](#)  
Get a fresh start with email that has less spam

 [Web History](#)  
Access and manage your web activity from any computer

 [iGoogle](#)  
Add news, games and more to the Google homepage

 [Google Checkout](#)  
A faster, safer and more convenient way to shop online

Sign in with your **Google Account**

Email:   
ex: pat@example.com

Password:

Stay signed in

[Can't access your account?](#)

**Don't have a Google Account?**  
[Create an account now](#)

# Google accounts

## Sign in to personalize your Google experience.

Google has more to offer when you sign in to your Google Account. You can customize pages, view recommendations, and get more relevant search results.

Sign in on the right or [create one for free](#) using just an email address and password you choose.



### [Gmail](#)

Get a fresh start with email that has less spam



### [Web History](#)

Access and manage your web activity from any computer



### [iGoogle](#)

Add news, games and more to the Google homepage



### [Google Checkout](#)

A faster, safer and more convenient way to shop online

Sign in (to  $\{to \$product\}$ ) with your

## Google Account

Email:

Password:

To sign in with this account, click Continue.

[About signing in](#)

Stay signed in

[Can't access your account?](#)

Don't have a Google Account?

[Create an account now](#)

# Google accounts

## Sign in to your organization's account at: **example.com**

This Google Account is administered by example.com. Google doesn't host the account and so doesn't know your password.

To sign in to this account from the Google Accounts page:

Type your full email address

Leave the password field blank

Click "Sign in"

You will be directed to the organization's sign-in page, where you can enter your password.



Sign in with your  
**Google Account**

Email:

Password:

Stay signed in

[Can't access your account?](#)

If you prefer to enter your username and password in one step, bookmark and use your organization's sign-in page.

[Sign in at example.com](#)

Search Photos

### Share photos with friends and family



### ...or explore public photos



### Sign in to Google

Google accounts

[Any Account](#)

Email

Password

.....

Stay signed in

[Can't access your account?](#)

[Learn more about Picasa Web Albums »](#)

### Also try Picasa 3

The next generation of Picasa: free software for organizing, editing and printing your photos.



[Download Picasa 3](#)



Search Photos

### Share photos with friends and family



### ...or explore public photos



[Learn more about Picasa Web Albums](#)

### Also try Picasa 3

The next generation of Picasa: free software for organizing, editing and printing your photos.



[Download Picasa 3](#)

### Sign in to Google

Google accounts

Any Account

For [alertblue.com](#) addresses, please login by clicking the 'Any Account' tab above, and then click 'Continue' after entering your email.

Email

Continue

Or pick from this list:

[Gmail](#)

[Yahoo! Mail](#)

[AOL Mail](#)

[Hotmail](#)

# Google as an OpenID RP

- Same problem as SAML: What does user type in Google's login box?
- New problem: How does the user signup?
  - Stage one: OpenID for email validation, not login
  - Stage two: UI improvements
- End Goal
  - Launch an RP to yahoo.com, hotmail.com, and aol.com to provide a large example site that others could mimic

## Account created. Please verify your current email address.

If you forget your password, Google can send you a link to ██████████@yahoo.com to reset it. [Learn more](#)

Verify by signing in at yahoo.com


This safe, secure verification is possible because Google and yahoo.com support [OpenID](#), which helps you verify that it's really you on participating websites.

If you would rather verify your account by email, [request an email verification](#)

**YAHOO!** Hi, Bryan ▾ | [Sign Out](#) | [Help](#)

Click "Agree" to sign in to www.google.com using your Yahoo! ID and allow sharing of Yahoo! info.

You are sharing the following:

 ██████████@yahoo.com

[Agree](#)

By clicking Agree you are agreeing to the [Yahoo! Additional Terms of Service](#).

Copyright © 2010 Yahoo! Inc. All rights reserved.  
[Copyright/IP Policy](#) | [Terms of Service](#) | [Guide to Online Security](#) | [Privacy Policy](#)

Search Photos

Share photos with friends and family



...or explore public photos



Sign in to Google

Google accounts

[Any Account](#)


Email

Choose a password:

Stay signed in

[Can't access your account?](#)

[Learn more about Picasa Web Albums »](#)

Latest news from the Google Photos Blog 

[Picasa Web Albums goes on a Picnik](#)

Tue Jul 13 2010

Picasa Web and Picnik A few months back we welcomed Picnik, the ...

[More posts](#)



Search Photos

### Share photos with friends and family



### ...or explore public photos



### Sign in to Google

Google accounts


Any Account

Email


Continue

Or pick from this list:

 [Gmail](#)

 [Yahoo! Mail](#)

 [AOL Mail](#)

 [Hotmail](#)

[Learn more about Picasa Web Albums »](#)

### Latest news from the Google Photos Blog

[Picasa Web Albums goes on a Picnik](#)

Tue Jul 13 2010

Picasa Web and Picnik A few months back we welcomed Picnik, the ...

[More posts](#)

# Detour One - Installed Apps

iPhone apps, POP/IMAP apps, Windows apps, Mac apps, Linux apps, Blackberry apps, etc.

- Google has no password for the user
- Same problem as OpenID & SAML: What does user type in the login box?
- On a web login page, we redirect via SAML/OpenID. What do you do from a login page that is not in a web-browser?

Hint: Try Tripit's iPhone/Android app, and login using a button



### Sign in to Web Albums

With Web Albums, you can share online photo albums with friends and family, or create public albums to share with the world. It's free, and easy to use.

[Click here to learn more.](#)

#### Sign in to Web Albums with your Google Account

Username:

Password:

Remember me on this computer

Sign In

Cancel


[Forgot your Password?](#)

[Sign up for Web Albums](#)

# Google™ Access Request

## Accounts

The **Photo Editor application on your computer** is requesting access to your Google Account for the product(s) listed below.

 **Picasa Web Albums** - <http://picasaweb.google.com>

If you grant access, you can revoke access at any time under 'My Account'. The Photo Editor application will not have access to your password or any other personal information from your Google Account. [Learn more](#)

**⚠** The application that directed you here claims to be "Photo Editor". We are unable to verify this claim as the application runs on your computer, as opposed to a website. We recommend you deny access unless you trust the application.

# Detour Two - Multi-factor auth

## Strong authentication

- keychain code generator
- SMS/phone-call
- hardware/software certificate, ...

## Similar problem

- On an installed app
- ..where user is not authenticated with a password
- Same problem as OpenID & SAML & Installed Apps: What does user type in the login box?

If we solve this problem in one use-case, we solve it for the other as well

- Big opportunity for mobile phone/network providers

# If we succeed, what next?

Assuming...

- IDPs provide functional and technical consistency
- OAuth2, OpenID, etc. evolve as expected
- Good RP best practices (including UI) are proven
- We have a solution for installed apps

Farther future involves scaling to more IDPs

- NASCAR UI + Email address
- long-tail IDP discovery: xauth.org, PDS/CDS, identity in the browser
- IDP quality: certification schemes, OIX, Kantara, InCommon, etc.

# Running an IDP for your business

## Short Answer

- Unless you are a Global 2000 firm, hire a SaaS vendor to do it for you

## Long Answer

- Login systems for Google, Facebook, MSFT, etc. have reliability > 99.99%
  - Can you run a system that reliably?
- Big identity providers have large security/identity teams keeping up with evolving best practices and security threats
  - Can you hire such a team?

## Business Value

- Control logins to your corporate blog, Facebook page, LinkedIn accounts, Google AdWords accounts, ...
- Extranet & Supply Chain scenarios

# Summary

- Industry has homework to do, but adoption is accelerating dramatically, and major players are heavily invested
- Most consumer websites should just watch this year, but plan for work in 2011
- Monitor for OpenID in the press
- Big opportunity for early market leaders in the consumer space who get this working well
  
- Enterprises should pick an IDP and experiment with extranet collaboration scenarios
- Enterprise SaaS vendors need to be aggressive - research SAML and Google Apps Marketplace