

A decorative header at the top of the slide features four overlapping spheres: a green one on the left, a blue one in the center, a red one to the right of the blue one, and a yellow one on the far right. A thin black horizontal line is positioned below the spheres.

Business value of Federated Login for

- **Enterprises**
- **Enterprise SaaS vendors**
- **Consumer websites**

Eric Sachs
Product Manager, Google Security & CIO
organization



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 RSA

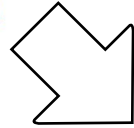
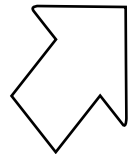


Google in 2003

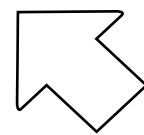
- Only a few thousand employees, but already using many SaaS vendors
- Nooglers introduced each week on Fridays
- Ops team manually provisions SaaS accounts
- Uh oh...
 - Mike was fired yesterday, and we forgot to go to each vendor and remove Mike's account, so he is still able to get in
 - We think Frank's password might have been stolen too, but its so much work to change it in all these places



Federated Login

A dark blue rectangular login form with a white "W" logo at the top. It contains the following text and fields: "Login" in white, "Username:" followed by a white input field, "Password:" followed by a white input field, a checkbox labeled "Remember me", and a "Login »" button at the bottom right.

Azure



Harder then it looks

Reliability?

- Ran in a single data center
- Ran on a single RAID server
- Not uncommon for login system to be inaccessible, while apps were still up

Security threat?

- Single-sign on systems on internal networks
- Federated login systems Internet accessible

Other Enterprises using Google Apps reported the same problems



Federated Login as a service

- Google noticed a growing set of Enterprises who were using an IDP SaaS service
 - Vendors such as Ping, Tricipher, Symplified, ...
- IDP services built many custom adapters for SaaS vendors
- Google wants to see better standards by SaaS vendors
- Launched [OpenID support for Google Apps](#) as another "IDP service"
 - Asking our corporate SaaS vendors to use OpenID



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](#)

Four options

1. Don't use a central login system
2. Deploy it yourself using enterprise software (Ping, Microsoft, Oracle, IBM, CA, etc.)
3. Outsource to an identity vendor (Ping, Symplified, Tricipher, etc.) who provides configuration for lots of SaaS vendors
4. Use Google Apps, but only with a subset of SaaS vendors



Moving beyond passwords

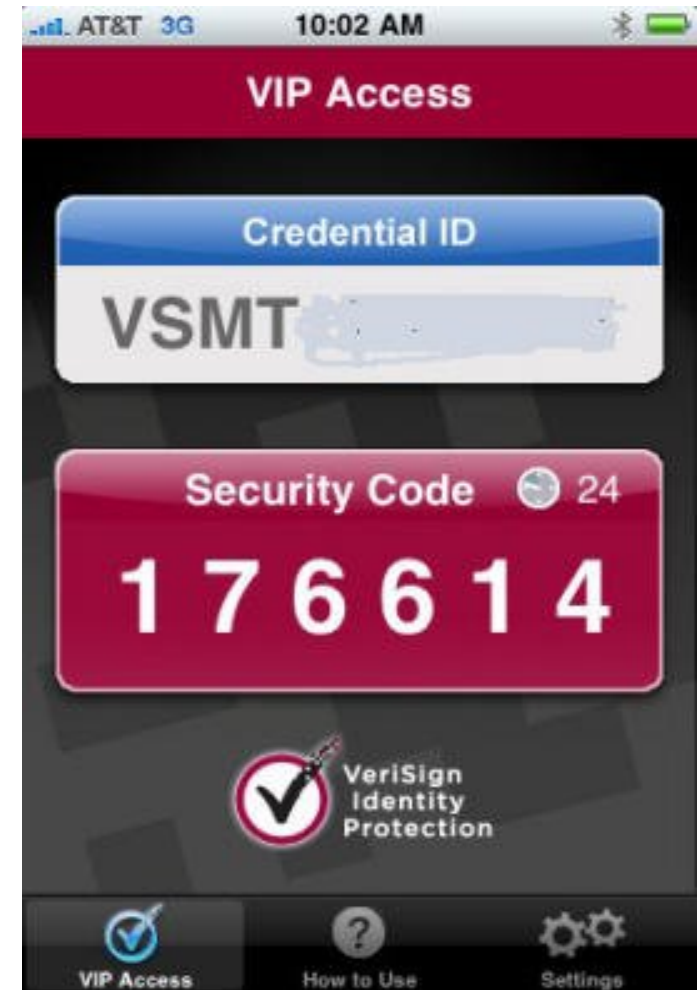
- Try adding stronger formats of authentication than passwords
- SaaS vendors have some very advanced methods to protect password hacking
 - ...but they can still be stolen or phished
- OTP=one time password generator



But I don't want to carry another device!

Usability is getting a lot better

Online banking uses similar models



Warning: Installed software

- Software on PCs and mobile devices
 - Example: POP, IMAP, Outlook
- Options
 - Machine generated passwords: Aldk3audD8
 - Blackberry Enterprise Server
 - Also supported by Google App Connector
 - Software that launches a web browser
 - Google Apps Sync for Outlook

What's next?

- We moved payroll, E-mail, and other business functions to the cloud
- We moved user identity/authentication to the cloud
- But what about all our backoffice IT apps?
 - New options: Amazon Web Service, Force.com, Microsoft Azure, Google App Engine
 - What new security issues does this raise?

Cloud security

- **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. (A service layer is needed to handle the security)
4. The technique needs to be an open industry standard, both to avoid lockin, and to get a detailed review by the security community



Welcome the crypto experts



- Industry standard: **OAuth**
 - Most Google & Yahoo APIs are OAuth enabled
 - But fails to meet need to hide all crypto from Enterprise IT developers
- November 2009: OAuth WRAP Profile announced by Microsoft, Google, & Yahoo
 - <http://www.google.com/group/oauth-wrap-wg>
 - Session SVC19 at Microsoft PDC09 conference
 - Early alpha testing of OAuth service in App Engine (already available for gadgets)
 - Facebook, Twitter, and others also have announced plans to use OAuth WRAP



OAuth available today

- WRAP profile not yet widely supported
- Many Enterprises already using OAuth for their IT apps in the cloud
- Many SaaS vendors already using OAuth for the web-service APIs they expose
 - Back to Google's IT department
 - How do we build IT apps to auto-add entries to Google calendars?
 - How do we monitor Google Docs for risky content?



Administrator in control



- Multiple enterprise systems can be **given access** to Google Apps APIs (including an AppEngine app)
- Each system can have different levels of access (calendar only, everything, etc.)
- Makes SaaS mashups possible as well
 - Example: SaaS vendor who provides a service for project management tracking
 - Task milestones can be pushed to Google Calendar
 - Administrator has to approve this access

Integration across SaaS vendors



[Home](#)

[Video Tour](#)

[Enterprise](#)

[Blog](#)

[Realtime News](#)

[about](#) | [contact us](#)

Login to your Socialwok

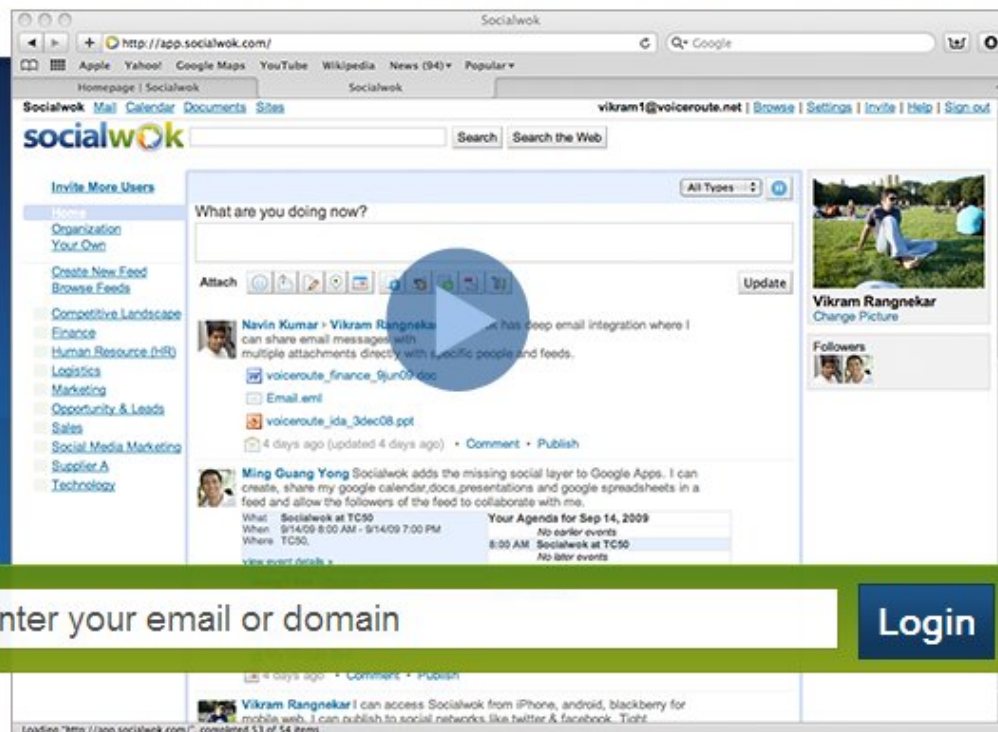
The missing Social App for Google Apps

Your own feed based social network in Google Apps to create and share links, Google Calender, Docs and more...

Login using Google Apps

enter your email or domain

Login



TechCrunch50 2009 Demo Pit Winner

Socialwok adds the missing social layer to Google Apps. Create a secure private social network for your Google Apps Domain.



SocialWok on Facebook

Become a Fan

And now for another perspective...

Security in "the cloud" for consumers



Security trends of 2008/2009

Webmail (Google/Yahoo/MSFT/etc.) providers getting nervous

- Webmail users reusing their passwords at other websites that get hacked, and expose those passwords
- Social network screen scraping of address books

Conclusion: Creating an industry solution for federated login would help security for webmail providers



UI brings sanity to OpenID

- Yahoo launches first with a UI that took 12 steps for a first time login
- Websites required a solution that INCREASED registration rates
- Facebook Connect launches a 1 step user interface

We've been busy

- OpenID foundation does first round of market research with large website owners
- Yahoo, Google, Facebook, AOL, and MSFT publicly share usability research at joint summits, and our independent results are all the same
- Addressed security issues in the protocol, including review/adoption by US Government



92% success rate

Plaxo managed to think "out of the box" and find a way to clearly improve usability by combining a few steps

Scenario:

- I sign up for Plaxo, and let them download my address book and send invitations to my friends, including a relative at rgsbsc@gmail.com
- Plaxo sends that relative an invitation, but sees he is a gmail.com user, and uses a special invitation...



Eric Sachs added you as a connection on Plaxo

Inbox | X

**Eric Sachs** to me[show details](#) 9:14 PM (0 minutes ago)

Reply



Eric Sachs wants to add you as a connection on Plaxo.

Message from Eric:
Lets sync up

To accept this connection request, go to:

<http://www.plaxo.com/invite?i=74435943&k=500926088&l=en>

Thanks!
The Plaxo team

More than 20 million people use Plaxo to keep in touch with the people they care about.
Don't want to receive emails from Plaxo any more? Go to: <http://www.plaxo.com/stop>

**Eric Sachs wants to connect with you on Pulse.**

Eric Sachs

To connect with Eric, join Plaxo.
And with express signup, you can use your Google account to join and find your friends in just a few clicks.

[Sign up with my Google Account](#)[Or, use another email address](#)

By clicking "Sign up with my Google Account", you are indicating you are over 13 years of age, agree to Plaxo's Terms, and agree to be included in the Plaxo Directory. We will not sell your information. [View our privacy policy.](#)

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](#)



Congratulations! Your account is ready to go.

X

In the future, click on the Google account link to sign in.



Sign In

E-mail:

Password:




Remember me


[Forgot password?](#)

Not a member yet?

Join over 20 million others who use Plaxo to stay in touch with the people they care about.

Other ways to sign in:

-  Sign in with OpenID
-  Sign in with Yahoo! ID
-  Sign in with a Google Account



Big success

- Increased registration success rate from 60% to 92%
 - Is that enough BUSINESS VALUE for you?
- Public announcement in Nov 09 on [Google Blog](#)
 - Facebook also using the technique to signup gmail users, many other websites planning to as well
 - @yahoo.com users can be registered using the same technique (Microsoft & AOL in the future)
- Does your company have a consumer facing website?



Q&A

Eric Sachs, Product Manager, Google Security
Chris Messina, Open Web Advocate

Slides available online

- Google search for "oauth goog" and click first result
- Search on the page for RSA

