

Google™



OpenID Single Sign On and OAuth Data Access for Google Apps

Ryan Boyd @ryguyrg

Dave Primmer

May 2010

Why?

**View live notes and questions about
this session on Google Wave:**

<http://bit.ly/magicwave>

Agenda

- Terminology
- History
- Open Protocols
 - OpenID user authentication
 - OAuth data access
 - Hybrid authentication + data access
- Google Apps Marketplace
- Case Study - Evolution of 'SaaSy Payroll'
- Q&A

SaaSy Payroll

SaaSy Payroll

- **Fictitious app** for handling the payroll of SMBs
- **Used by** smart-lawfirm.com for their payroll



SaaSy Payroll
your payroll solution, your way

Payroll

Your Paycheck for 5/1/2010

You've worked a lot this week: **74 hours**
Your hourly rate is: **\$12**

Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

Future Pay Dates:
5/8/2010
5/15/2010
5/22/2010
5/29/2010

Terminology

Authentication and Authorization

- **Authentication**

- Goal: Secure knowledge of the identity of the user

- **Authorization**

- Goal: Appropriate access to resources, such as Google Data APIs (Calendar, Contacts, Docs, etc)

History

History (2001-2005)

2001

2002

2003

2004

2005

OpenID
5/2005

History (2006-2010)

ClientLogin
4/2006

2006

2007

2008

2009

2010

History (2006-2010)

ClientLogin
4/2006

2006

2007

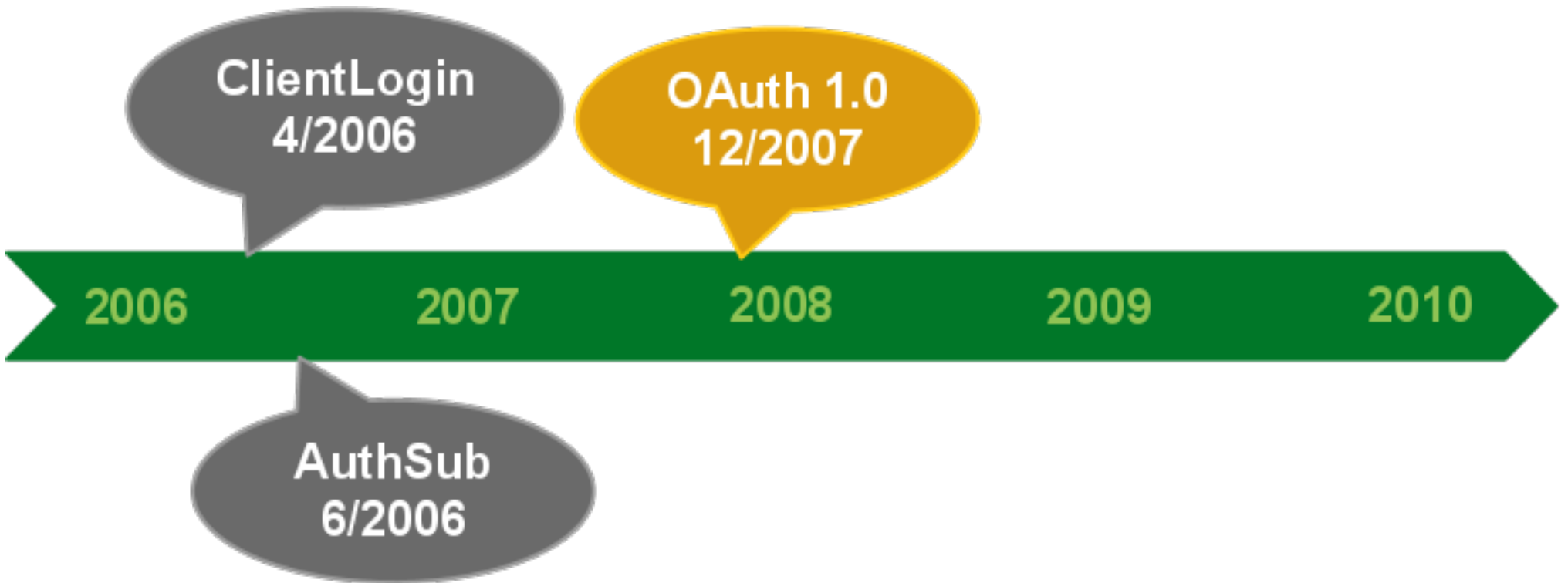
2008

2009

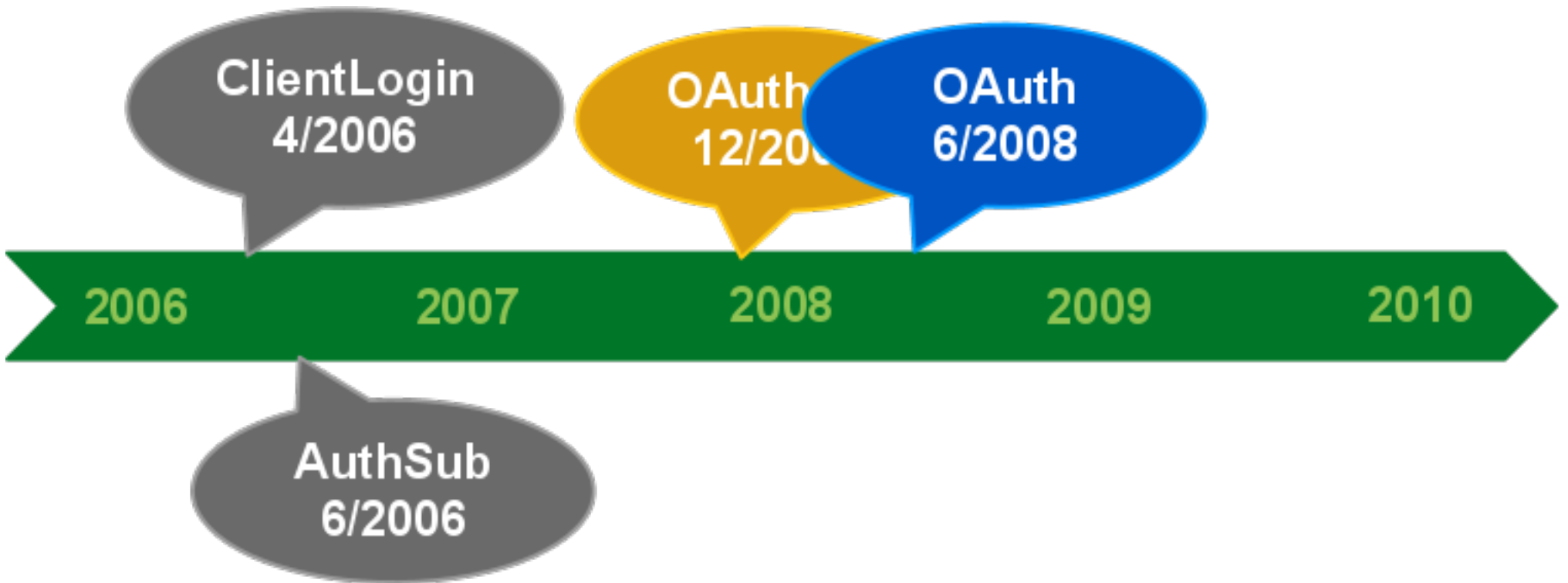
2010

AuthSub
6/2006

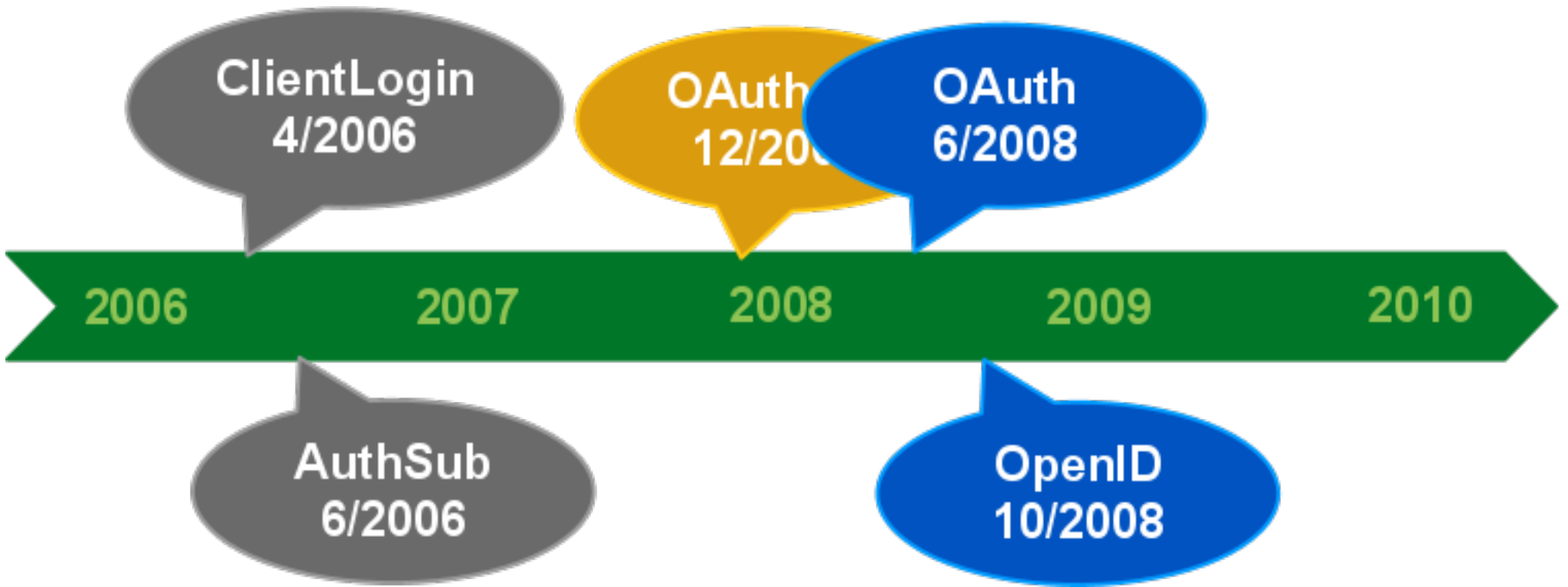
History (2006-2010)



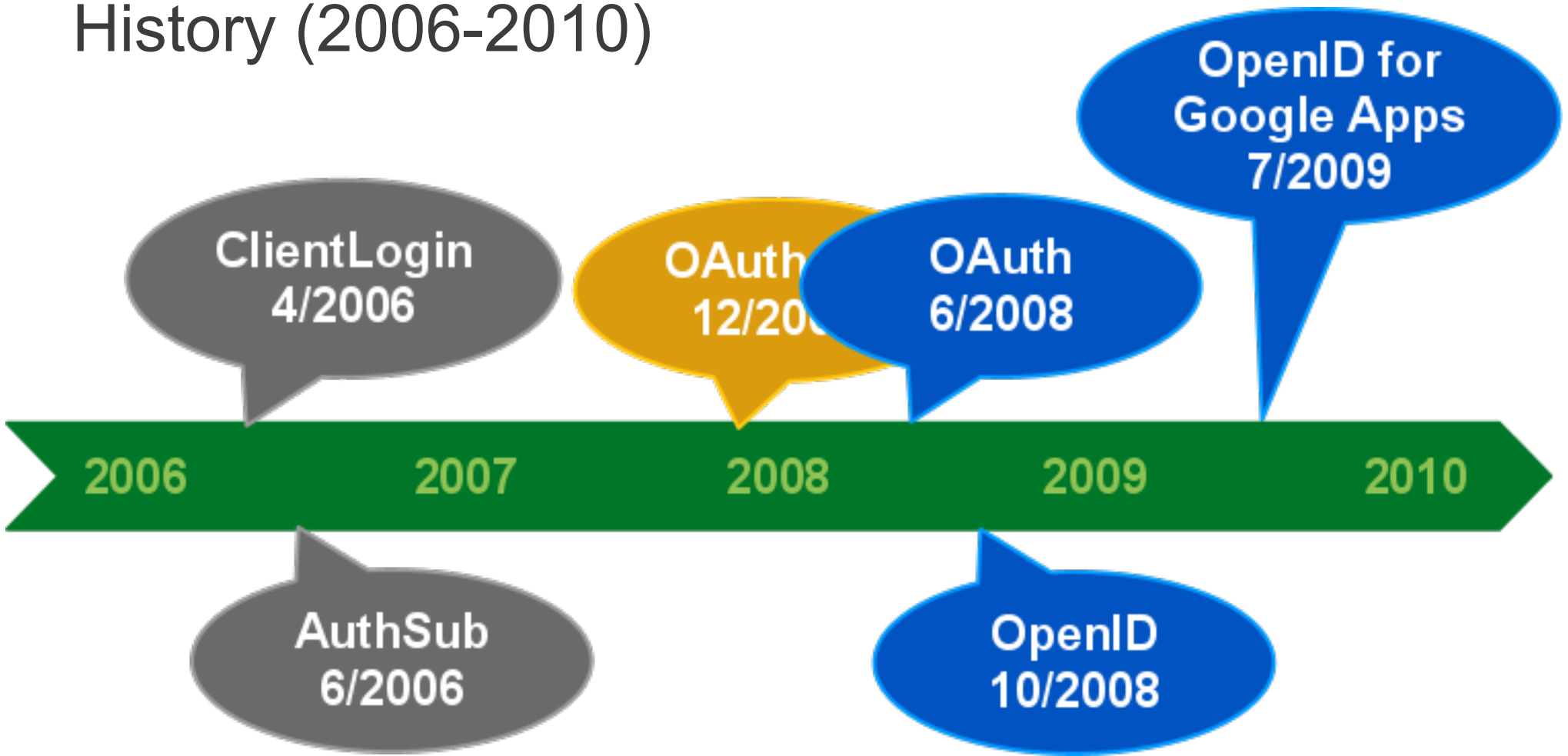
History (2006-2010)



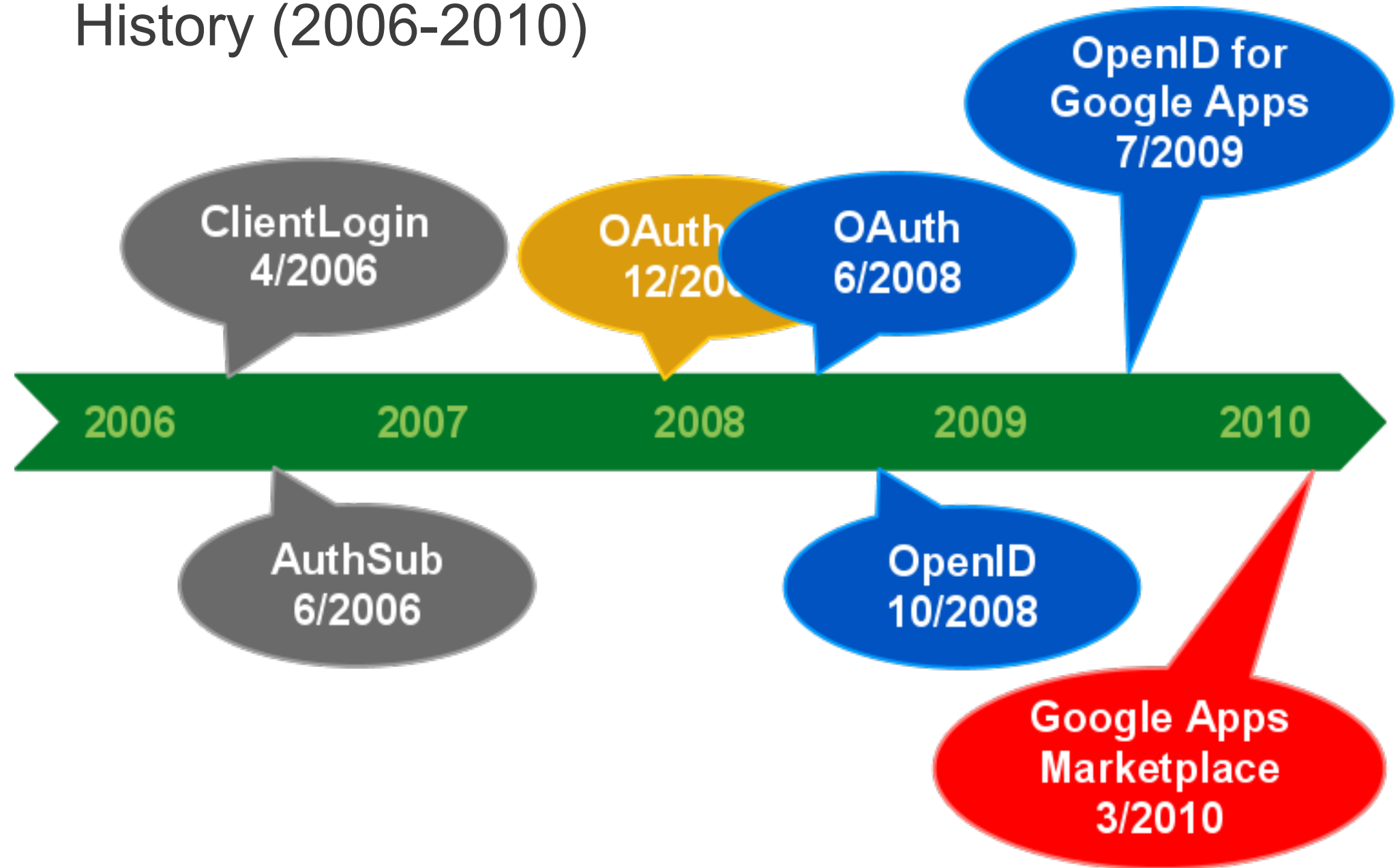
History (2006-2010)



History (2006-2010)



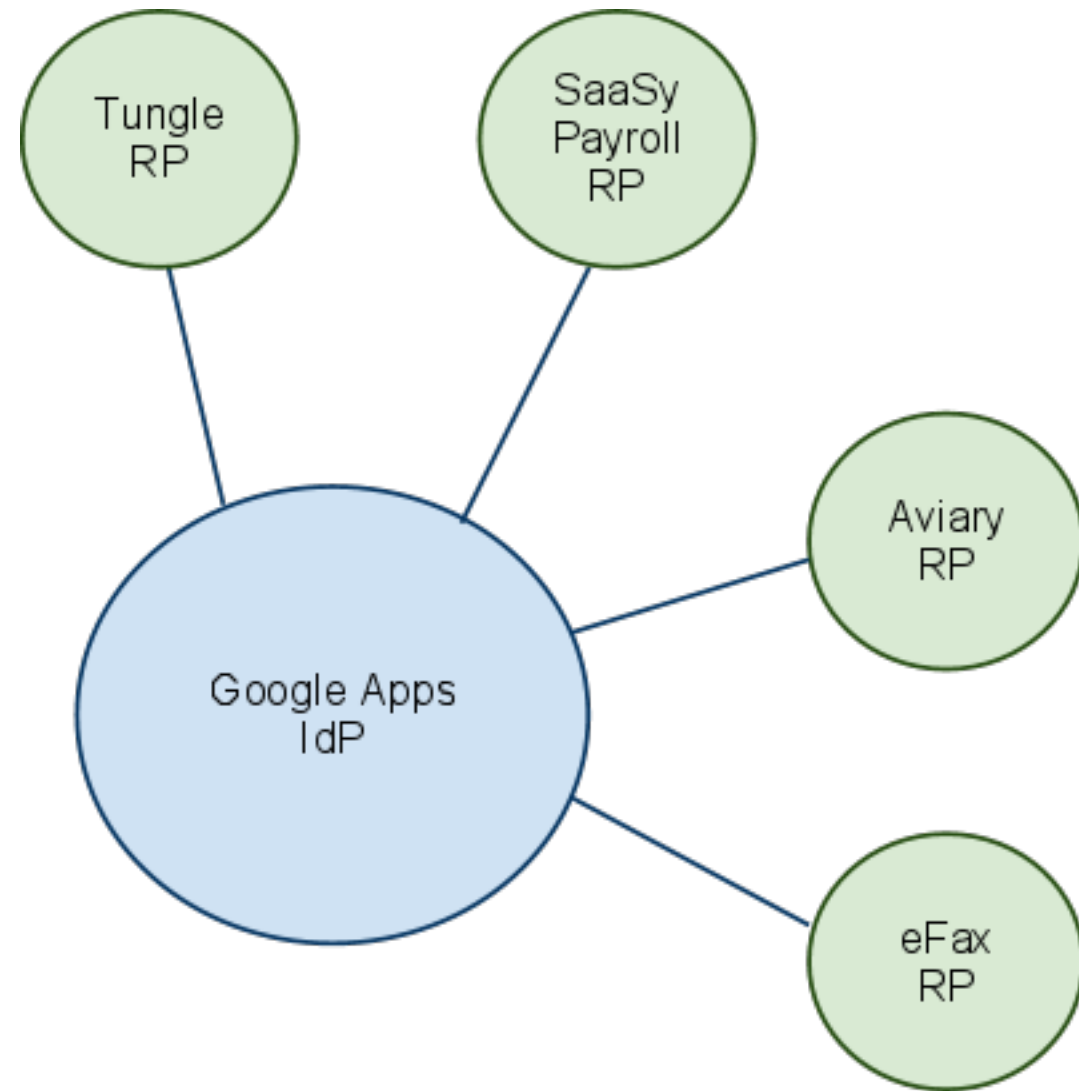
History (2006-2010)



OpenID Federated Identity

What do we mean by Federated Identity?

Web applications (relying parties) accept the assertion of identity from identity providers, such as Google and Yahoo.



What information does OpenID provide an app?

- **Identity** of the user:
<http://smart-lawfirm.com/openid?id=0123456789>
- **Static** each time the user visits the relying party web application

"OpenID is a **safe, faster, and easier** way to log in to web sites."

openid.net

Safe, Faster and Easier

- **Safe**

- The user only enters their credentials one place:
on the website of their OpenID provider

- **Faster**

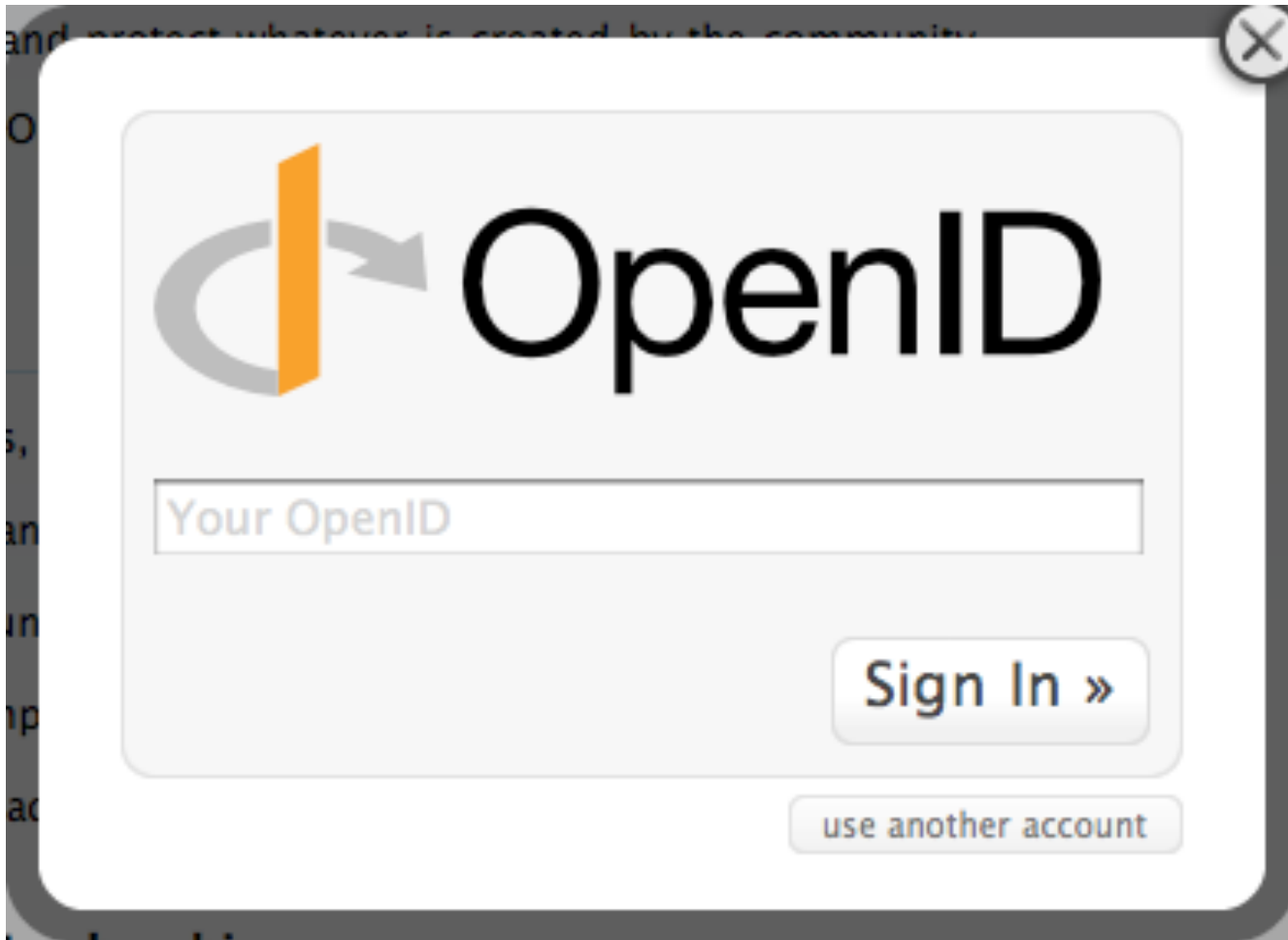
- The user is often already logged into their
OpenID provider

- **Easier**

- The user no longer needs to create and maintain
a new account and credentials on every web site

Discovery: Determining the OpenID provider for a user.

OpenID Login Options



and protect whatever is created by the community

O

5,

an


in

op

ac

L

11

 **OpenID**

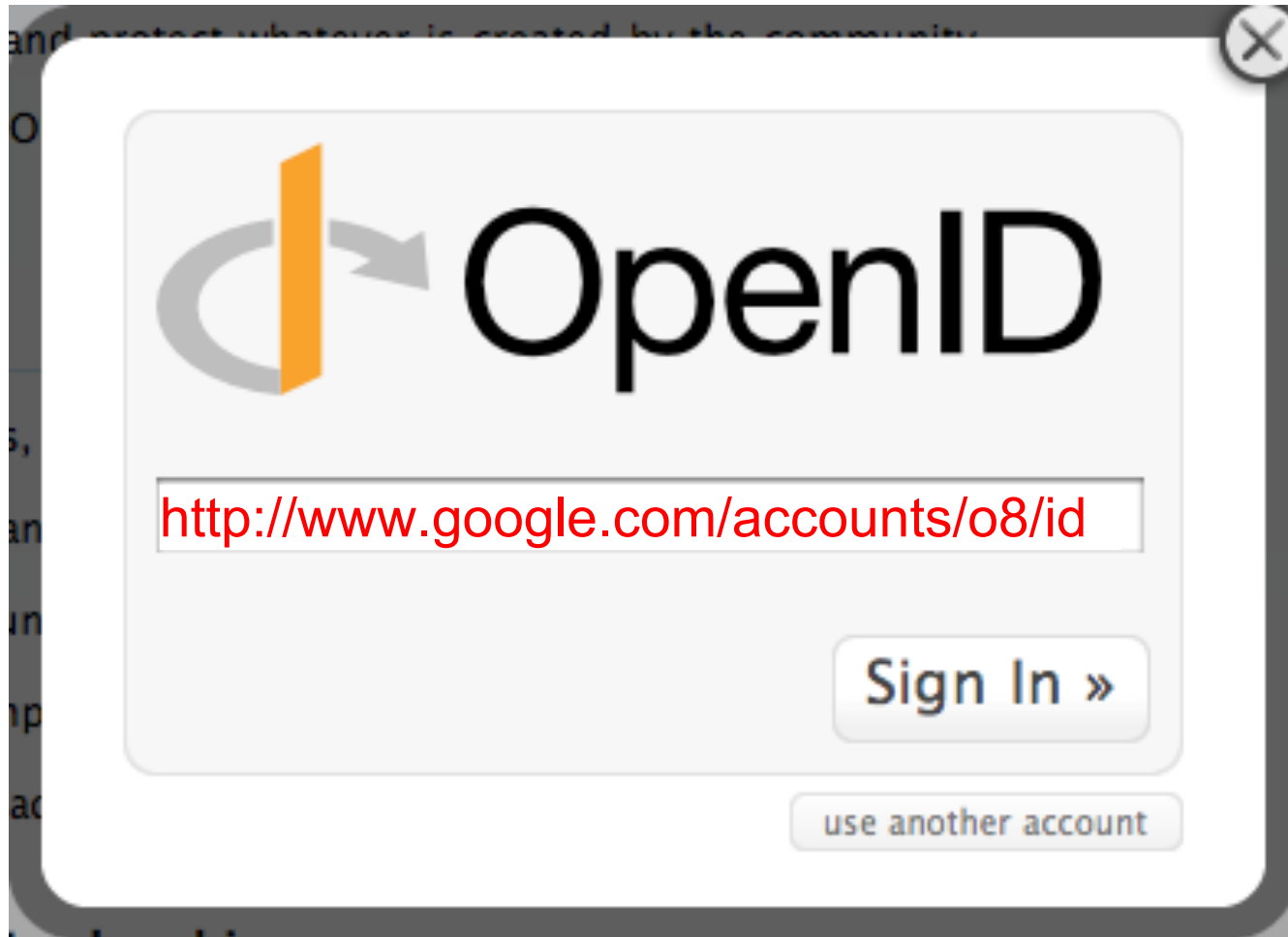
Your OpenID

Sign In »

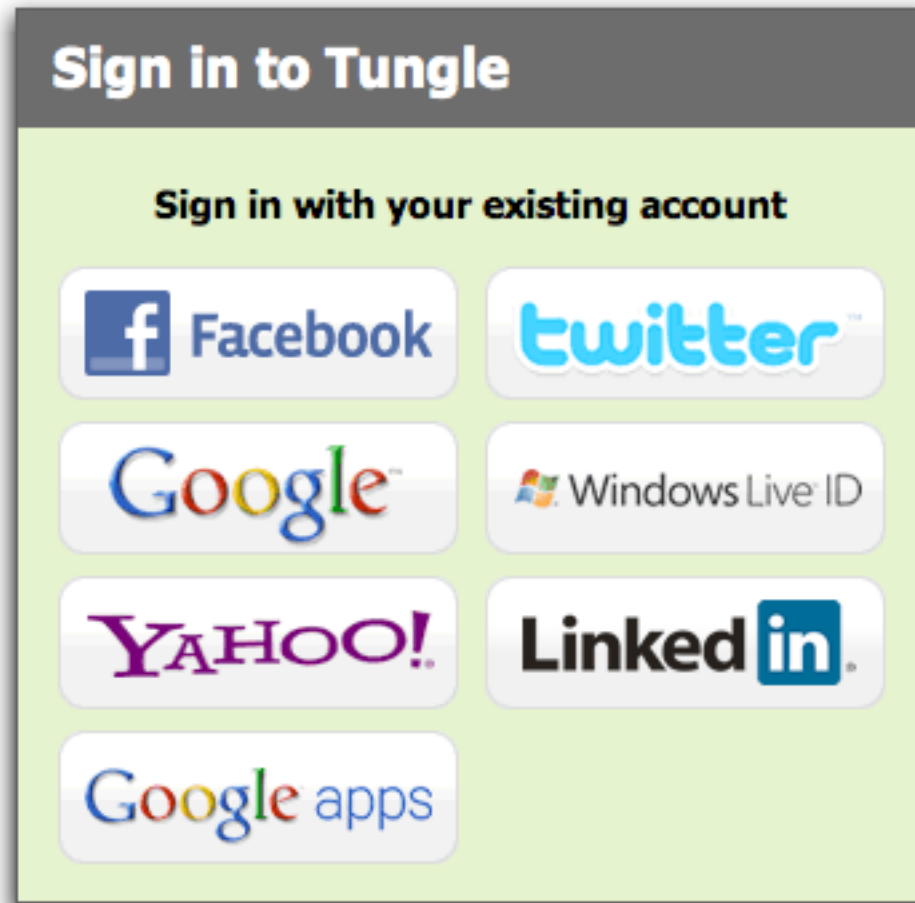
use another account

The image shows a modal dialog box for OpenID login. It features the OpenID logo (a grey 'C' shape with an orange vertical bar and a grey arrow) and the text 'OpenID' in a large, bold, black font. Below the logo is a text input field with the placeholder text 'Your OpenID'. To the right of the input field is a button labeled 'Sign In »'. Below the 'Sign In' button is a smaller button labeled 'use another account'. The dialog box has a grey border and a close button (an 'X' in a circle) in the top right corner. The background behind the dialog box is a blurred screenshot of a webpage with some text visible.

OpenID Login Options



Improved UX



OpenID Demo with a Gmail account

The screenshot shows the Manymoon website interface. At the top left is the Manymoon logo. To the right is a login form with a "Remember me" checkbox, "Email" and "Password" input fields, a "Forgot Your Password?" link, and a "LOGIN" button. Below the login form is a link that says "Login using Google or Google Apps". The main content area features a large headline: "the easiest and **FREE** way to simplify your worklife!". Below the headline are two lines of text: "★★★★★ Top Rated App for Google Apps" and "Trusted By Tens of Thousands of Businesses". A video player is embedded in the center, showing a video titled "Manymoon" with a play button in the center. The video player has a progress bar at the bottom showing "0:00 / 1:44". To the right of the video player is a section titled "Get work done" with three bullet points: "+ Eliminate hundreds of emails per person per week!", "+ 'I love Manymoon's clean design, customizability, ease of use and its focus on teams and tasks.' Alexandra Samuel, Principal, Social Signal", and "+ Integrate Google Apps into conversations, group projects, tasks and events". At the bottom right of this section is a large orange button that says "Join Now, it's FREE!".

Remember me

Forgot Your Password?

Email

Password

LOGIN

Login using Google or Google Apps

manymoon

the easiest and **FREE** way to simplify your worklife!

★★★★★ Top Rated App for Google Apps

Trusted By Tens of Thousands of Businesses

Manymoon

Get work done

- + Eliminate hundreds of emails per person per week!
- + "I love Manymoon's clean design, customizability, ease of use and its focus on teams and tasks." Alexandra Samuel, Principal, Social Signal
- + Integrate Google Apps into conversations, group projects, tasks and events

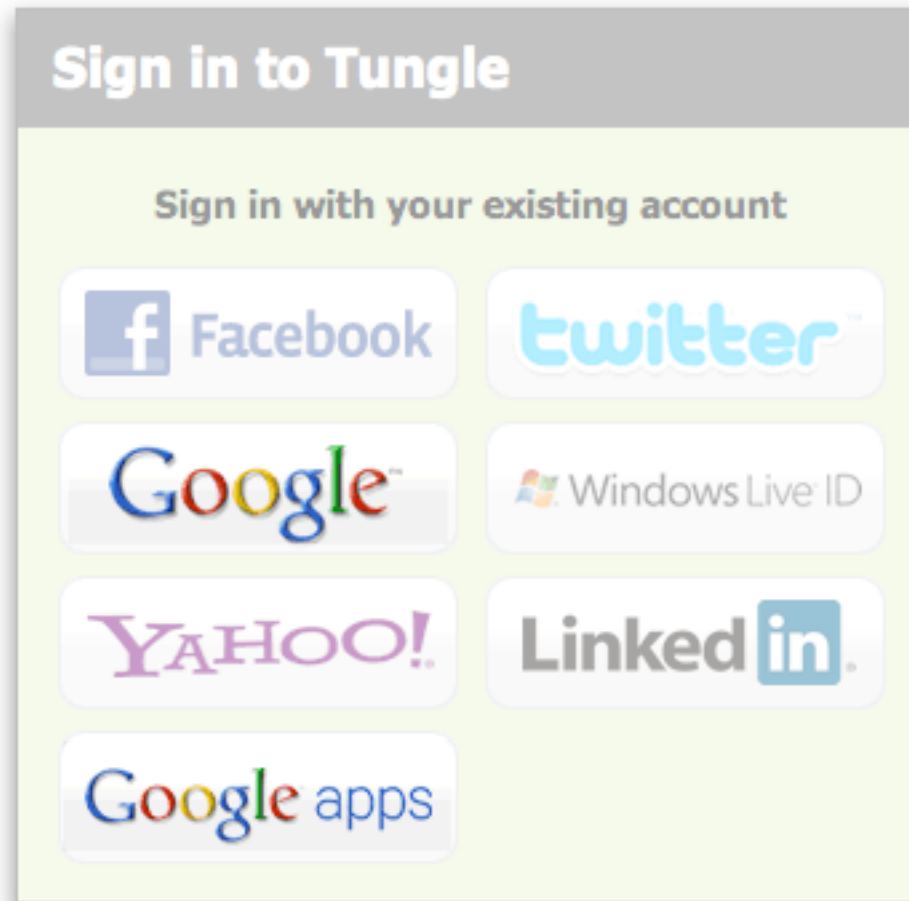
Join Now, it's FREE!

But... what if you want to use an
OpenID on **your own domain**
without a complicated URL to
remember?


Ideal User Experience: WebFinger

What is your e-mail address?

Google Accounts versus Google Apps accounts



Google Apps Login

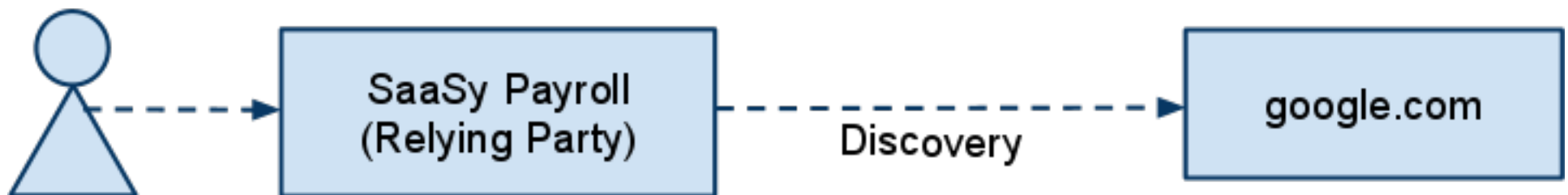
To sign in to  Google Apps please enter your
GoogleApps domain:
 [Sign in](#)

Discovering the OpenID Provider

- 1 Attempt discovery on smart-lawfirm.com directly



- 2 Check if smart-lawfirm.com outsourced discovery to google.com



Format of the OpenID Identity

- **Google consumer account (including Gmail accounts):**
<https://www.google.com/accounts/o8/id?id=AItOawlTW-qs7L-bpYc0oxROHDQaFmQHyGRnaLM>
- **Google Apps account:**
<http://smart-lawfirm.com/openid?id=0123456789>

Supported Extensions

- **Provider Auth Policy Extension (PAPE)**
 - Allows a relying party to ask for security restrictions
- **OpenID User Interface Extension**
 - Enables pop-up UI
- **OAuth Hybrid**
 - Enables getting both the user's identity and access to some of the user's data
- **Attribute Exchange (AX)**
 - Provides additional info about the user

Attribute Exchange (AX)

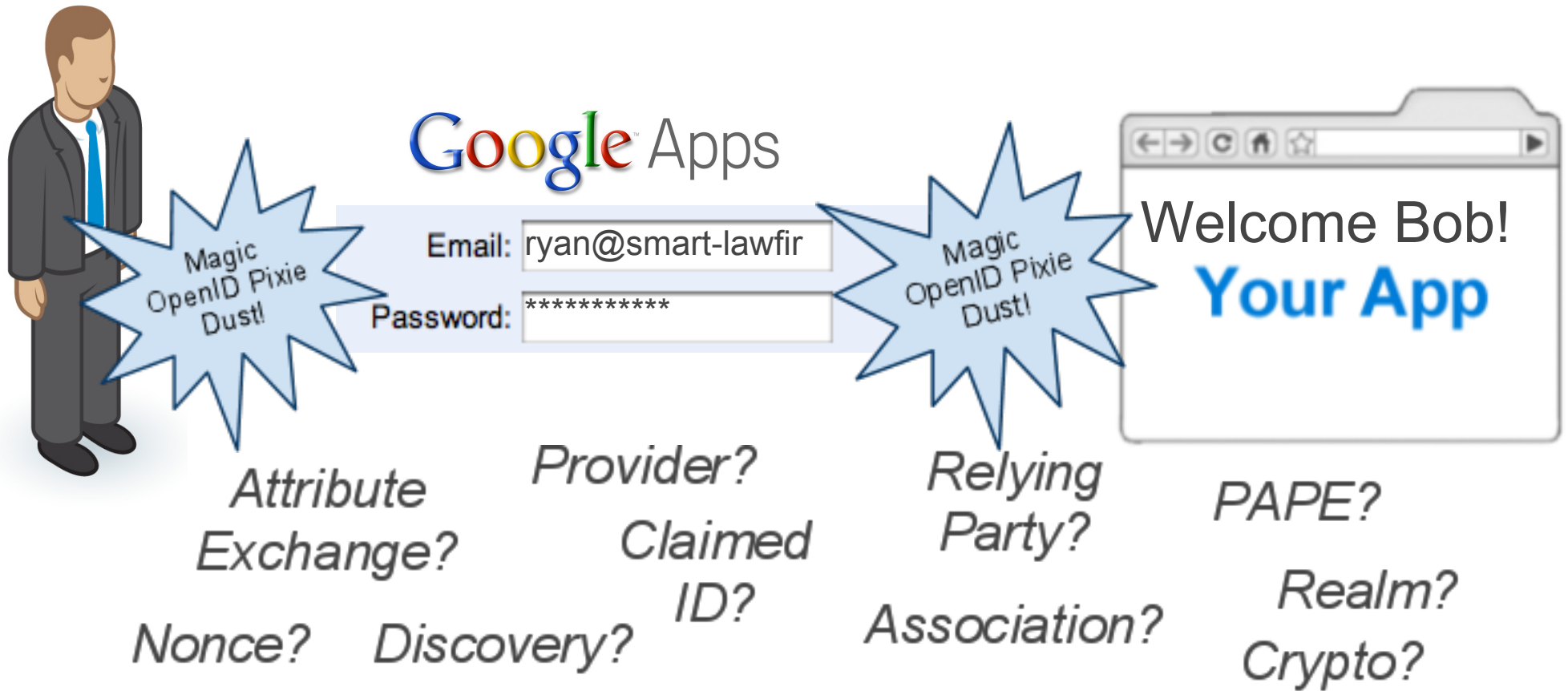
- **Remember**, without AX we only get a URI:
<http://smart-lawfirm.com/openid?id=0123456789>
- **We want more** information to improve the user experience
 - First Name
 - Last Name
 - E-mail Address
 - Language

Attribute Exchange (AX) Trust

- Don't trust attributes without verification
 - Whitelist trusted IDPs
 - Same-origin policy for email
 - One-time confirmation messages

How it's done - OpenID Federated Identity

OpenID Federated Identity



Sounds complicated, but not hard in practice!

OpenID Libraries

Language	Libraries
Java	OpenID4Java, Step2
.NET	DotNetOpenAuth
PHP	php-openid, php-openid-apps-discovery
Ruby	ruby-openid, ruby-openid-apps-discovery
Any	RPX, Ping Identity

OAuth Data Access



OAUTH

OAuth Terms

- **Protected Resource**
 - resides on server
 - requires authorization



**Protected
Resource**

OAuth Terms

- **Protected Resource**
 - resides on server
 - requires authorization



Protected Resource

- **Resource Owner**
 - owns protected resource
 - approves access



Resource Owner

OAuth Terms

- **Protected Resource**
 - resides on server
 - requires authorization
- **Resource Owner**
 - owns protected resource
 - approves access
- **Server**
 - receives http request



Protected Resource

Google calendar

Server



Resource Owner

OAuth Terms

- **Protected Resource**
 - resides on server
 - requires authorization
- **Resource Owner**
 - owns protected resource
 - approves access
- **Server**
 - receives http request
- **Client**
 - makes http request



Protected Resource



Resource Owner



Server



Client

Old OAuth Terminology

Pre 2009		Current
Consumer	→	Client
Service Provider	→	Server / Protected Resource
User	→	User / Resource Owner

More Info: [The Authoritative Guide to OAuth 1.0](#)

Now, with more RFC! <http://www.rfc-editor.org/info/rfc5849>

OAuth Components

Key Management

- Establishes trust between client and server

Access Control

- Grants done per-user, or for a whole Google Apps domain.


Basic steps to use OAuth

Step 1 Client Registration <- Key Management

Step 2 Resource owner grant <- Access Control

Step 3 Client Application Accesses resource

SaaSy App - www.saasyapp.com



The screenshot shows a web browser window with the address bar displaying <http://www.saasyapp.com/payroll.php>. The page title is "SaaSy Payroll" with the tagline "your payroll solution, your way". A red button labeled "Payroll" is visible. The main content area displays "Your Paycheck for 5/1/2010" and states "You've worked a lot this week: 74 hours" and "Your hourly rate is: \$12". A table lists payroll items and their amounts. Below the table, "Future Pay Dates" are listed as 5/8/2010, 5/15/2010, 5/22/2010, and 5/29/2010, with a link to "Add dates to your Google Calendar".

SaaSy Payroll
your payroll solution, your way

Payroll

Your Paycheck for 5/1/2010

You've worked a lot this week: **74 hours**
Your hourly rate is: **\$12**

Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

Future Pay Dates:
5/8/2010
5/15/2010
5/22/2010
5/29/2010

[Add dates to your Google Calendar](#)

SaaSy App - www.saasyapp.com

SaaSy Payroll

your payroll solution, your way

Payroll

Your Paycheck for 5/1/2010

You've worked a lot this week: **74 hours**
Your hourly rate is: **\$12**

Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

Future Pay Dates:
5/8/2010
5/15/2010
5/22/2010
5/29/2010

[Add dates to your Google Calendar](#)

Step 1 - For the Developer:

Getting your OAuth client key and secret

A Google Client App Registration Page

My Account

https://www.google.com/accounts/b/0/UpdateDomain

[My Account](#) | [Help](#) | [Sign out](#)

Google accounts

Manage **www.saasyapp.com** (Active)

To register your domain, provide the following information. Once you've registered with an authentication certificate, you will be able to use secure tokens when communicating with a Google service.

Target URL path prefix:
Must be the prefix of the *next* parameter used in AuthSub.
e.g. <http://example.com/authsub>

Domain description (Optional):
Tell us about your domain

OAuth Consumer **www.saasyapp.com**
Key:

OAuth Consumer **cB7fg1x94QAcEva**
Secret:

We do not have a certificate for your domain.

Upload new X.509 cert: No file chosen
(Optional) File must be in PEM format. [Learn More](#)

Step 2 - For the Resource Owner: Access Control



Two types of Access Control

Resource Owner: An entity capable of approving access to a protected resource.

- Sometimes the resource owner is not the same as the user

<p>Consumer</p> 		<p>Business</p> 
<p>Individual User is Resource Owner</p>		<p>Company Admin is Resource Owner</p>

Two types of Access Control

<h2>Three-Legged OAuth</h2>		<h2>Two-Legged OAuth</h2>
<h3>Consumer</h3> 		<h3>Business</h3> 
<p>Individual User is Resource Owner</p>		<p>Company Admin is Resource Owner</p>

Two types of Access Control

Three-Legged OAuth		Two-Legged OAuth
Authorization using browser redirection		Requests pre-authorized for a group of users
Individual prompted		User not prompted

Approval for a group of users:

Manage OAuth Client Data Access

Google Apps Administrator Access Control

The screenshot shows a web browser window with the Google Apps interface. The address bar displays the URL <https://www.google.com/a/cpanel/smart-lawfirm.com/ManageOauthClients>. The page header includes the Google Apps logo, the text "Google Apps for smart-lawfirm.com - Premier Edition", the user email "admin@smart-lawfirm.com", and links for "Inbox", "Calendar", "Help", and "Sign out". Below the header is a navigation menu with tabs for "Dashboard", "Users and groups", "Domain settings", "Advanced tools" (which is selected), "Support", and "Service settings-". A "Back to Advanced tools" link is also present.

Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [Learn more](#)

Authorized API clients The following API client domains are registered with Google and authorized to access data for your users.

Client Name	One or More API Scopes	Actions
<input type="text"/> Example: www.example.com	<input type="text"/> Example: http://www.google.com/calendar/feeds/ (comma-delimited)	<input type="button" value="Authorize"/> Learn more about registering new API clients
SaaSy Voice	Docs (Read/Write) https://docs.google.com/feeds/ To export a call log	<input type="button" value="Remove"/>
	Contacts (Read/Write) https://www.google.com/m8/feeds/ To display names of people who called	

At the bottom of the page, there are links for "Terms of Service", "Privacy policy", "Suggest a feature", and "Google Home", along with the copyright notice "©2010 Google Inc."

Google Apps Administrator Access Control

Google Apps for smart-lawfirm.com - Premier Edition **admin@smart-lawfirm.com** [Inbox](#) [Calendar](#) [Help](#) [Sign out](#)

Search accounts Search Help Center **Resource Owner**

Dashboard Users and groups Domain settings **Advanced tools** Support Service settings-

[« Back to Advanced tools](#)

Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [Learn more](#)

Authorized API clients The following API client domains are registered with Google and authorized to access data for your users.

Client Name **One or More API Scopes** [Learn more about registering new API clients](#)

Example: www.example.com Example: http://www.google.com/calendar/feeds/ (comma-delimited)

Client

SaaSy Voice	Docs (Read/Write) https://docs.google.com/feeds/ To export a call log	Remove
	Contacts (Read/Write) https://www.google.com/m8/feeds/ To display names of people who called	

[Terms of Service](#) - [Privacy policy](#) - [Suggest a feature](#) - [Google Home](#)
©2010 Google Inc.

Google Apps Administrator Access Control

The screenshot shows the Google Apps Administrator interface for the domain smart-lawfirm.com. The user is logged in as admin@smart-lawfirm.com, identified as the Resource Owner. The page is titled "Manage API client access" and provides instructions on how to authorize API clients. A table lists authorized clients and their permissions. Two red circles highlight the "Client Name" field (www.saasyapp.com) and the "One or More API Scopes" field (http://www.google.com/calendar/feeds/), which are collectively labeled as the Protected Resource.

Google Apps for smart-lawfirm.com - Premier Edition
admin@smart-lawfirm.com | Inbox | Calendar | Help | Sign out
Resource Owner

Dashboard | Users and groups | Domain settings | **Advanced tools** | Support | Service settings-
« Back to Advanced tools

Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [Learn more](#)

Authorized API clients The following API client domains are registered with Google and authorized to access data for your users.

Client Name	One or More API Scopes	Authorize
www.saasyapp.com Example: www.example.com	http://www.google.com/calendar/feeds/ Example: http://www.google.com/calendar/feeds/ (comma-delimited)	Learn more about registering new API clients

Client

SaaSy Voice	Docs (Read/Write) https://docs.google.com/feeds/ To export a call log	Remove
	Contacts (Read/Write) https://www.google.com/m8/feeds/ To display names of people who called	

Protected Resource

[Terms of Service](#) - [Privacy policy](#) - [Suggest a feature](#) - [Google Home](#)
©2010 Google Inc.

Google Apps Administrator Access Control

The screenshot shows the Google Apps Administrator interface for the domain smart-lawfirm.com. The page is titled "Manage API client access" and provides instructions on how to manage API clients. Below the instructions, there is a section for "Authorized API clients" which lists several clients. Two clients are circled in red: "SaaSy App!" and "Calendar (Read/Write)".

Manage API client access
Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [Learn more](#)

Authorized API clients The following API client domains are registered with Google and authorized to access data for your users.

Client Name	One or More API Scopes	Actions
<input type="text"/> Example: www.example.com	<input type="text"/> <input type="button" value="Authorize"/> Example: http://www.google.com/calendar/feeds/ (comma-delimited)	Learn more about registering new API client
SaaSy App!	Calendar (Read/Write) https://www.google.com/calendar/feeds/	Remove
SaaSy Voice	Docs (Read/Write) https://docs.google.com/feeds/ To export a call log	Remove
	Contacts (Read/Write) https://www.google.com/m8/feeds/ To display names of people who called	Remove

Step #3 Access the resource

Demo: Two-Legged OAuth cURL

Two-Legged OAuth

What is it?

- An authenticated HTTP request. Very much like HTTP Digest Auth.
- Client has a role account name and password:
 - **consumer_key** -> account name
 - **consumer_secret** -> password
- Request param to indicate the user
 - **xoauth_requestor_id=ryan@smart-lawfirm.com**
- Some request attributes are bundled up and signed in a standard way. That's it.

Two-Legged OAuth

Why?

- You don't want to bother the user with approval
- The common Enterprise IT scenario
- Server to Server -- no browser involved
- Main trust relationship:
 - Resource Owner (admin) tells the Server, via ACL to trust the client
 - Permission stored in server ACL, not a token

The "other" style of authorization

Three-legged OAuth

Three-Legged OAuth

What is it?

- Describes the access control *delegation* to a Client by a Resource Owner
- Redirection-Based Authorization
 - The authorization flow is what most people think of when they talk about OAuth. It is the process in which the user's browser is redirected to the server to approve access

Three-Legged OAuth

What is it?

- Adds an Access Token to the 2LO request during data access that identifies the permission granted.

"Joe gives the SaaSy Payroll client permission to write to Joe's Google Calendar."

`oauth_token=1%2FSTnrUiu8N4OQvrwEpsltnpYwFX5an2j2i-VAK5l_3No`

SaaSy App - www.saasyapp.com

The screenshot shows a web browser window with the address bar displaying <http://www.saasyapp.com/payroll.php>. The page title is "SaaSy Payroll" with the tagline "your payroll solution, your way". A red button labeled "Payroll" is visible. The main content area displays "Your Paycheck for 5/1/2010" and states "You've worked a lot this week: 74 hours" and "Your hourly rate is: \$12". A table lists payroll items and their amounts:

Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

Below the table, "Future Pay Dates:" are listed as 5/8/2010, 5/15/2010, 5/22/2010, and 5/29/2010. A link "Add dates to your Google Calendar" is provided at the bottom.

SaaSy App - www.saasyapp.com

SaaSy Payroll

your payroll solution, your way

Payroll

Your Paycheck for 5/1/2010

You've worked a lot this week: **74 hours**
Your hourly rate is: **\$12**

Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

Future Pay Dates:
5/8/2010
5/15/2010
5/22/2010
5/29/2010

[Add dates to your Google Calendar](#)


Authorization by Resource Owner

My Account

ryan@smart-lawfirm.com | [My Account](#) | [Sign out](#)

Google accounts

The site www.saasyapp.com is requesting access to your Smart-lawfirm.com account for the product(s) listed below.

 **Calendar** - <http://calendar.smart-lawfirm.com>

If you grant access, you can revoke access at any time under 'My Account'. www.saasyapp.com will not have access to your password or any other personal information from your Smart-lawfirm.com account.

Authorization by Resource Owner

The screenshot shows a web browser window with the address bar containing the URL: <https://www.google.com/a/smart-lawfirm.com/AuthSubRequest?next=http://www.saasyapp.com/payroll.ph>. The page header includes the text "My Account" and the email address "ryan@smart-lawfirm.com" with links for "My Account" and "Sign out". The main content features the "Google accounts" logo and the text "The site www.saasyapp.com is requesting access to your Smart-lawfirm.com account for the product(s) listed below." Below this, a red oval highlights the text "Calendar - <http://calendar.smart-lawfirm.com>". At the bottom, there are two buttons: "Grant access" and "Deny access".

Client

User / Resource Owner

Protected Resource

Three-Legged OAuth

Why?

- Appropriate for access grant by individual user
 - (Also works for Apps users)
- User identity is opaque to client application
- Main trust relationship:
 - User is the Resource Owner and trusts the client app with an Access Token

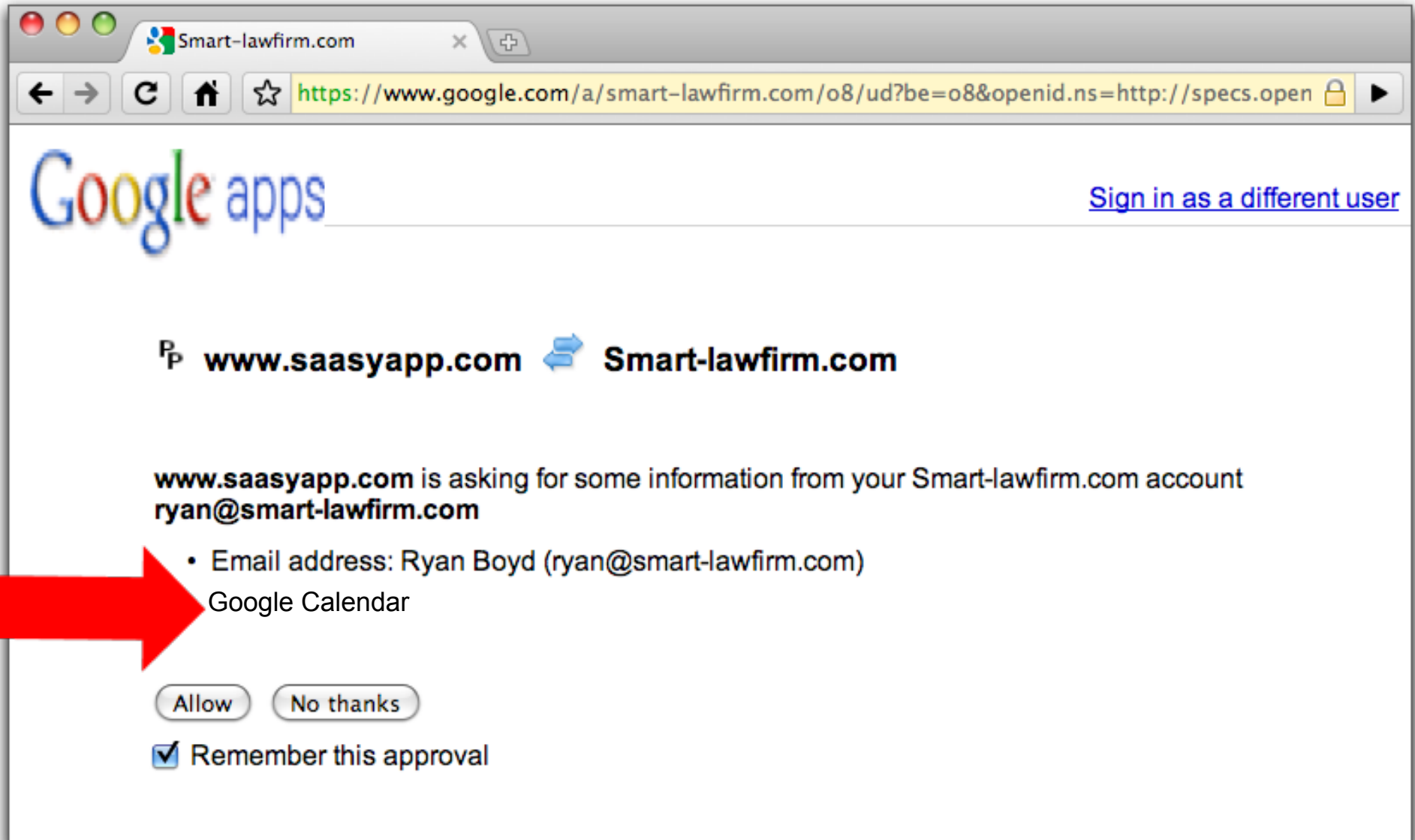
OAuth 2

- Already? Why?
 - Make it IETF standard
 - Add new use cases
 - Avoid crypto!
- OAuth 1 + WRAP = OAuth 2
- Facebook has working OAuth 2 prototypes, Microsoft Azure and Google have WRAP prototypes.
- <http://tools.ietf.org/html/draft-ietf-oauth-v2>


Hybrid OpenID + OAuth

Hybrid OpenID + OAuth

- Identity and Data Access in 1 step



Hybrid OpenID + OAuth

 Print			Day	Week	Month	4 Days	Agenda
Thu	Fri		Sat				
29	30		May 1				
6	7		8				
			Pay Day! 📅				
13	14		15				
			Pay Day! 📅				

Google Apps Marketplace

Features: Simple installation flow

Google Apps Marketplace Accounting & Finance Search Marketplace

Marketplaces

Google Apps > Accounting & Finance

SaaSy Payroll
your payroll solution, your way

SaaSy Payroll
by [SaaSy App Company](#) ★★★★★

Provides payroll service for your business. Everyone gets paid!

Provides payroll service for your business. Everyone gets paid!

Recent Customer Reviews no reviews
This product has no reviews yet.

Add it now [Learn more](#)

Pricing Details
\$10/user/month

Specifications

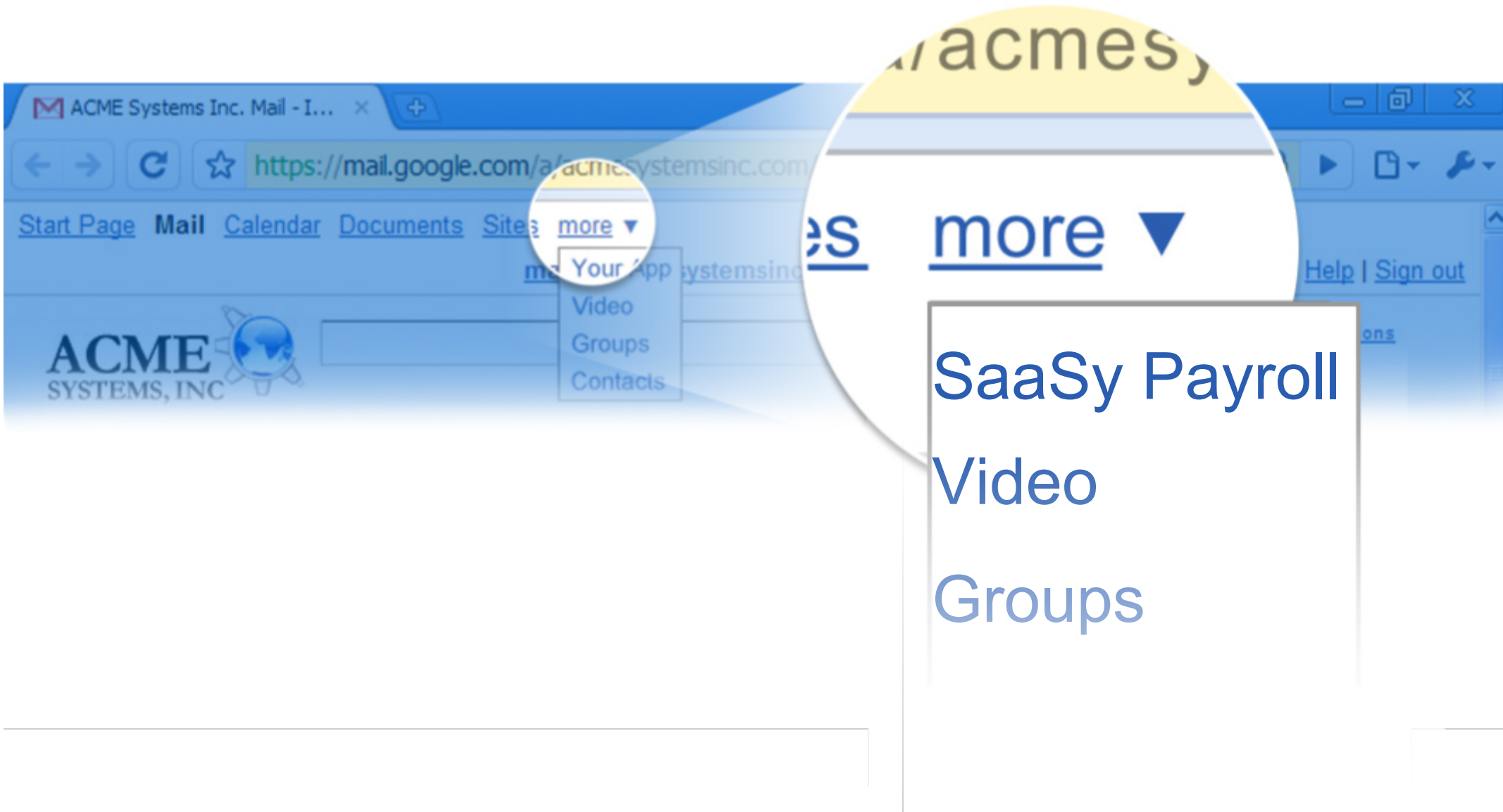
Data access requirements

- Calendar (Read/Write, does ...)

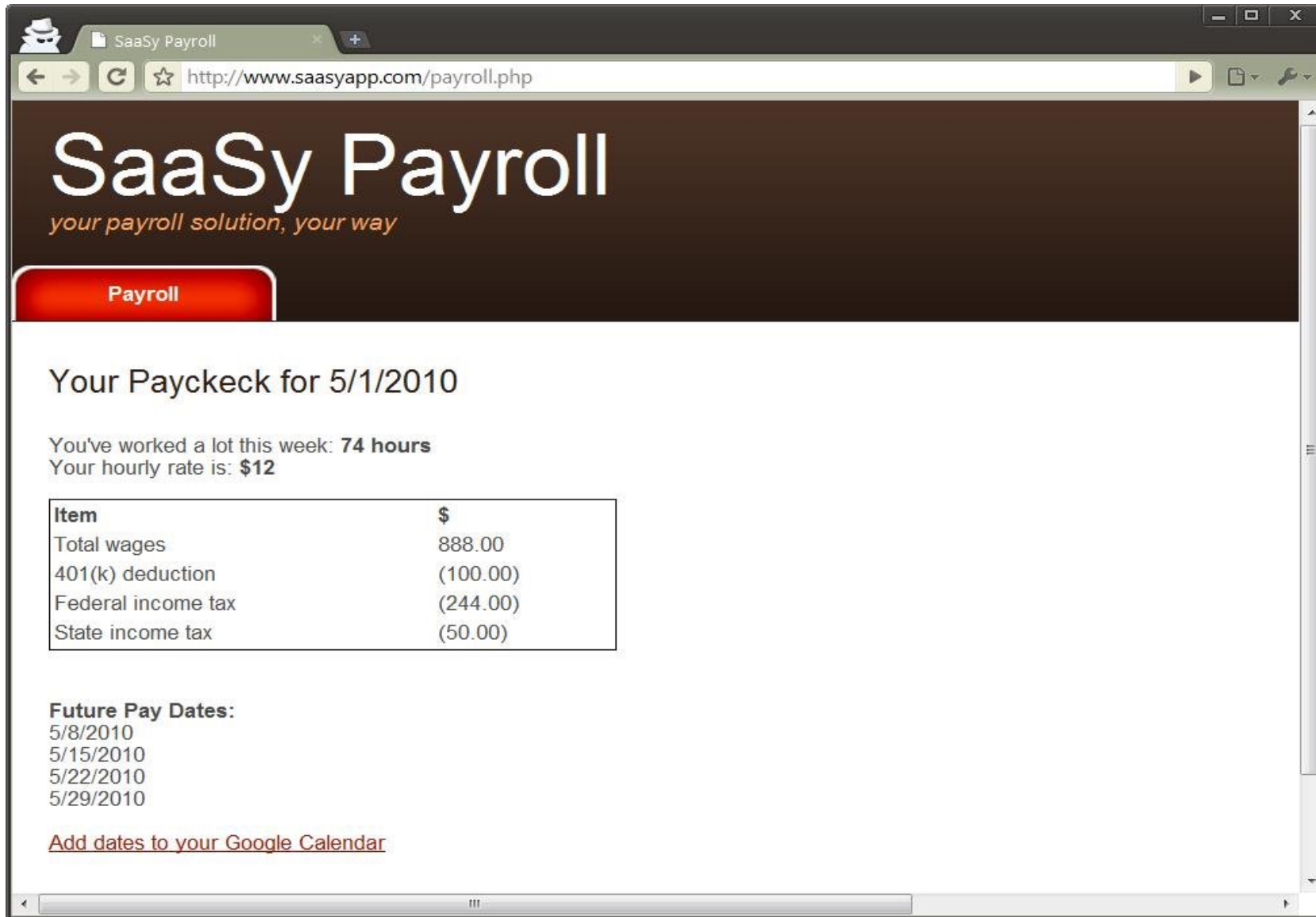
About the Vendor

[SaaSy App Company](#)
1600 Amphitheatre Parkway
Mountain View
94043
United States
[Vendor website](#)

Features: True Single Sign On



Features: True Single Sign On



The screenshot shows a web browser window with the address bar displaying <http://www.saasyapp.com/payroll.php>. The page title is "SaaS Payroll" with the tagline "your payroll solution, your way". A red button labeled "Payroll" is visible. The main content area displays "Your Paycheck for 5/1/2010" and states "You've worked a lot this week: 74 hours" and "Your hourly rate is: \$12". Below this is a table with two columns: "Item" and "\$". The table lists "Total wages" (888.00), "401(k) deduction" (100.00), "Federal income tax" (244.00), and "State income tax" (50.00). At the bottom, there is a section for "Future Pay Dates:" listing 5/8/2010, 5/15/2010, 5/22/2010, and 5/29/2010, with a link to "Add dates to your Google Calendar".

SaaS Payroll
your payroll solution, your way

Payroll

Your Paycheck for 5/1/2010

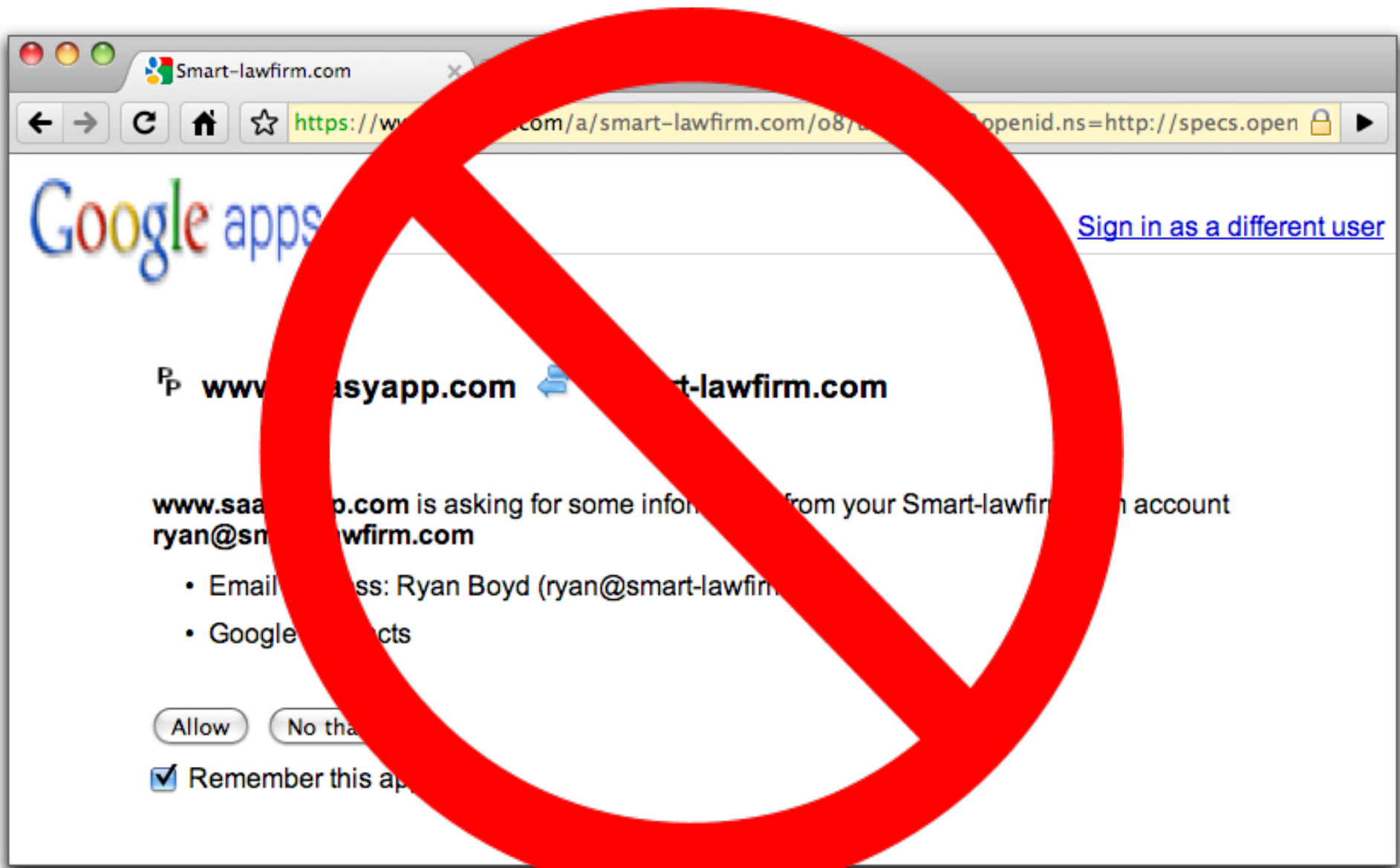
You've worked a lot this week: **74 hours**
Your hourly rate is: **\$12**

Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

Future Pay Dates:
5/8/2010
5/15/2010
5/22/2010
5/29/2010

[Add dates to your Google Calendar](#)

Features: True Single Sign On



Features: 2-legged OAuth access to Data APIs

The screenshot shows a web browser window with two tabs: 'Smart-lawfirm.com' and 'Google Apps'. The address bar displays the URL: <https://www.google.com/a/cpanel/smart-lawfirm.com/DomainAppInstall>. The page title is 'Google Apps for smart-lawfirm.com - Premier Edition'. The user is logged in as 'admin@smart-lawfirm.com'. The navigation menu includes 'Dashboard', 'Users and groups', 'Domain settings', 'Advanced tools', 'Support', and 'Service settings-'. A prominent message states: 'You have requested that the ' SaaSy Voice ' service be added to your domain'. Below this, the 'Grant data access' step is highlighted, showing a progress bar with four steps: 1 Agree to terms, 2 Grant data access, 3 External configuration, and 4 Enable the app. A warning message states: 'In order to work properly, this app needs to access your domain's data. It will be able to access the data exposed by Google APIs, which may include reading, writing, or deleting the data described below. Only grant data access to applications that you trust.' The permissions listed are: 'User Provisioning (Read only)' (To get a list of users to provision accounts), 'Docs (Read/Write)' (To export a call log), and 'Contacts (Read/Write)' (To display names of people who called). On the right, an 'App Overview' box for 'SaaSy Voice' includes a link to 'View in the marketplace' and lists features: 'Includes: - Google universal navigation - Single Sign-On through OpenID'. At the bottom, there are two buttons: 'Grant data access' and 'Cancel'.

Smart-lawfirm.com Google Apps

<https://www.google.com/a/cpanel/smart-lawfirm.com/DomainAppInstall>

Google Apps for smart-lawfirm.com - Premier Edition admin@smart-lawfirm.com [Inbox](#) [Calendar](#) [Help](#) [Sign](#)

Google apps Search accounts Search Help Center

Dashboard Users and groups Domain settings Advanced tools Support Service settings-

You have requested that the ' SaaSy Voice ' service be added to your domain

Grant data access

1 Agree to terms 2 Grant data access 3 External configuration 4 Enable the app

In order to work properly, this app needs to access your domain's data. It will be able to access the data exposed by Google APIs, which may include reading, writing, or deleting the data described below. **Only grant data access to applications that you trust.**

- User Provisioning (Read only)**
To get a list of users to provision accounts
- Docs (Read/Write)**
To export a call log
- Contacts (Read/Write)**
To display names of people who called

App Overview

SaaSy Voice [View in the marketplace](#)

SaaSy Voice

Includes:

- Google universal navigation
- Single Sign-On through OpenID

Grant data access Cancel

Features: 2-legged OAuth access to Data APIs


- Consumer Key and Secret available in the Marketplace

developer@saasyapp.com | My Vendor Profile | [Help](#) | [Feedback](#) | [Sign Out](#)

Google Apps Marketplace

Marketplaces ▾

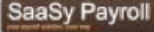
SaaSy App Company Inc.




1600 Amphitheatre Parkway
Mountain View
94043
United States
[Vendor website](#)

[Developer resources](#)

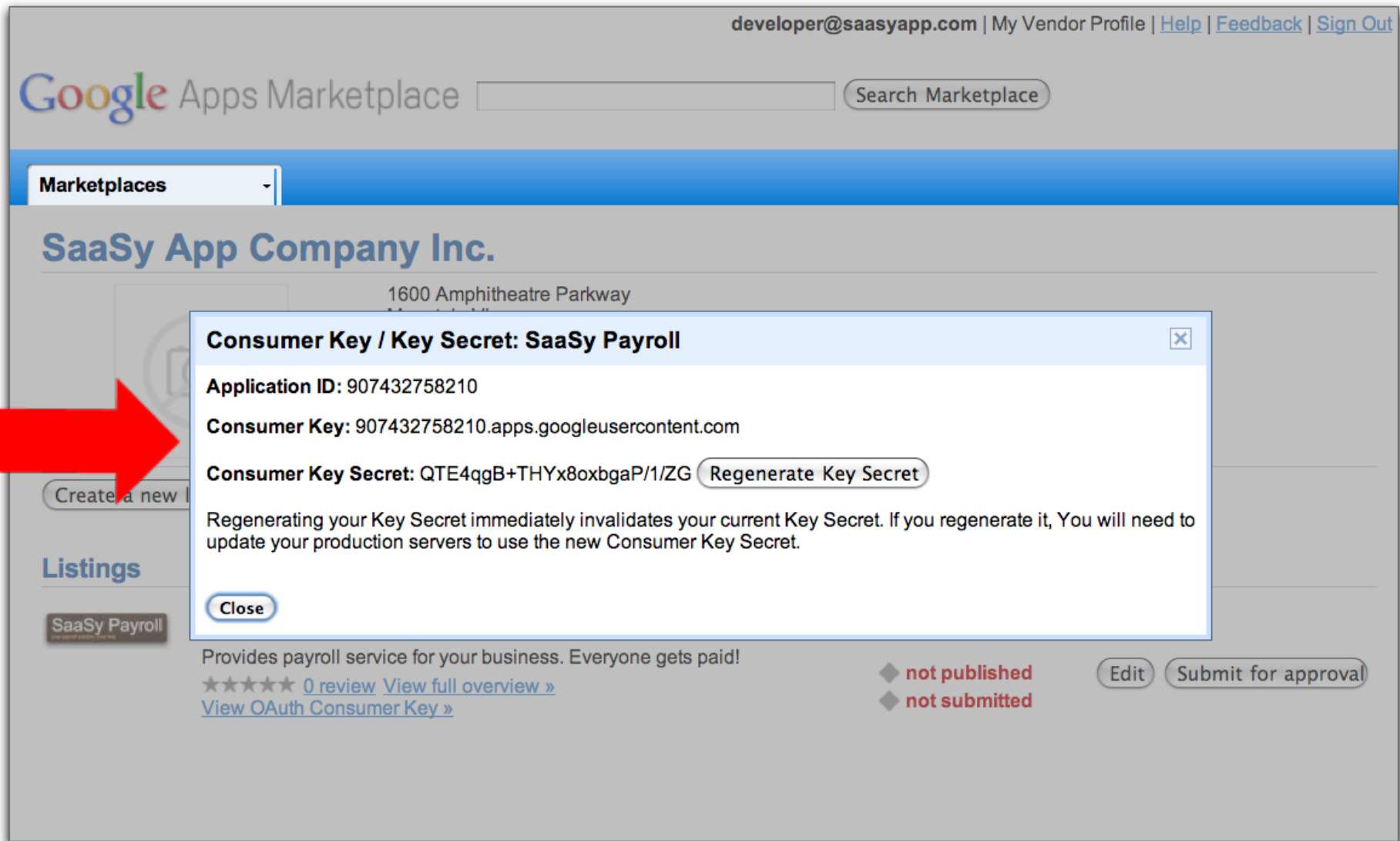
Listings

	SaaSy Payroll Provides payroll service for your business. Everyone gets paid! ★★★★★ 0 review View full overview » View OAuth Consumer Key »	Listing status ◆ not published ◆ not submitted	<input type="button" value="Edit"/> <input type="button" value="Submit for approval"/>
---	--	---	--



Features: 2-legged OAuth access to Data APIs

- Consumer Key and Secret available in the Marketplace



The screenshot shows the Google Apps Marketplace interface for a developer. At the top right, the user is logged in as 'developer@saasyapp.com' with links for 'My Vendor Profile', 'Help', 'Feedback', and 'Sign Out'. The main header includes the 'Google Apps Marketplace' logo and a search bar. A blue navigation bar contains a 'Marketplaces' dropdown menu. The main content area displays the profile for 'SaaSy App Company Inc.' with the address '1600 Amphitheatre Parkway'. A modal dialog box is open, titled 'Consumer Key / Key Secret: SaaSy Payroll'. It contains the following information: 'Application ID: 907432758210', 'Consumer Key: 907432758210.apps.googleusercontent.com', and 'Consumer Key Secret: QTE4qgB+THYx8oxbgaP/1/ZG'. A 'Regenerate Key Secret' button is next to the secret. Below this, a warning states: 'Regenerating your Key Secret immediately invalidates your current Key Secret. If you regenerate it, You will need to update your production servers to use the new Consumer Key Secret.' A 'Close' button is at the bottom left of the modal. In the background, the 'SaaSy Payroll' listing is visible, showing a 'Create a new listing' button, a 'Listings' section, and the app's name 'SaaSy Payroll'. The app description reads: 'Provides payroll service for your business. Everyone gets paid!'. It has '0 review' and a link to 'View full overview'. There are also links for 'View OAuth Consumer Key', 'not published', and 'not submitted' status indicators. 'Edit' and 'Submit for approval' buttons are at the bottom right of the listing area.

Summary of Protocols

Summary of Protocols

ClientLogin	Don't use for new apps
AuthSub	Don't use for new apps
3-Legged OAuth	Access data for individual users
2-Legged OAuth	Access data for an entire Google Apps domain
OpenID	Access a user's identity. Can be used for Gmail
OpenID with Google Apps extensions	Access a user's identity for Google Apps accounts
OpenID / OAuth Hybrid	On-board new users and get their data in one step

Evolution of an Integrated App

Evolution of 'SaaSy Payroll'

2006

2007

2008

2009

2010

email	password
john@foo.com	AxNAAFSnz



SaaSy Payroll

your payroll solutions, your way



New Customer Form

First Name:	<input type="text" value="Ryan"/>
Last Name:	<input type="text" value="Bond"/>
E-mail address:	<input type="text" value="ryan@smart-lawfirm.com"/>
Password:	<input type="password" value="***"/>
Confirm Password:	<input type="password" value="**"/>



Evolution of 'SaaSy Payroll'



AuthSub

email	password	token
john@foo.com	AxNAAFSnz	ZD1FNKL4

Google accounts

The site www.saasyapp.com is requesting access to your Smart-lawfirm.com account for the product(s) listed below.

-  Calendar - <http://calendar.smart-lawfirm.com>

If you grant access, you can revoke access at any time under 'My Account'. www.saasyapp.com will not have access to your information from your Smart-lawfirm.com account.



Evolution of 'SaaSy Payroll'



email	password	openid	token
john@foo.com	AxNAAFSnz	-----	ZD1FNKL4
jane@goo.com	-----	http://goo.com/1234	JFNB2ANS

Your Paycheck for 5/1/2010

You've worked a lot this week: 74 hours
Your hourly rate is: \$12

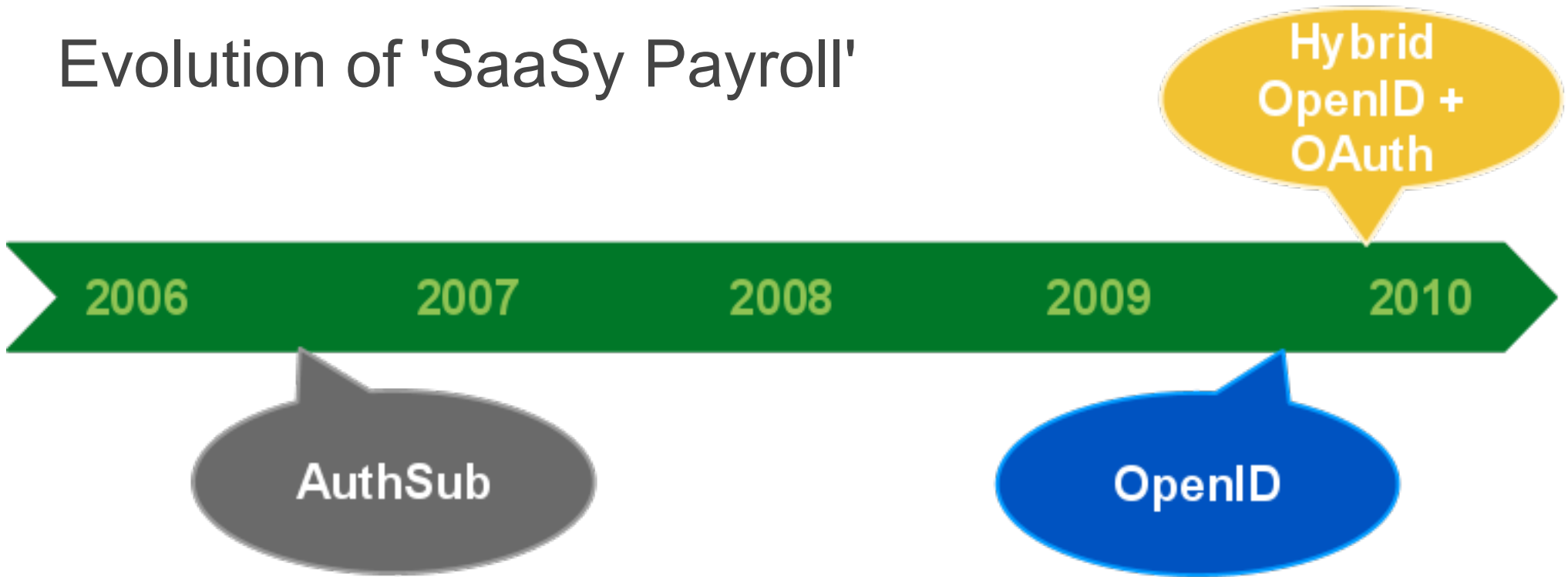
Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

Future Pay Dates:

5/8/2010
5/15/2010
5/22/2010
5/29/2010

[Add dates to your Google Calendar](#)

Evolution of 'SaaSy Payroll'



email	password	openid	token	type	secret
john@foo.com	AxNAAFSnz	-----	ZD1FNKL4	AS	-----
jane@goo.com	-----	http://goo.com/1234	JFNB2ANS	AS	-----
alan@bar.com	-----	http://bar.com/6780	D2FNAF7D	3LO	adfa123f



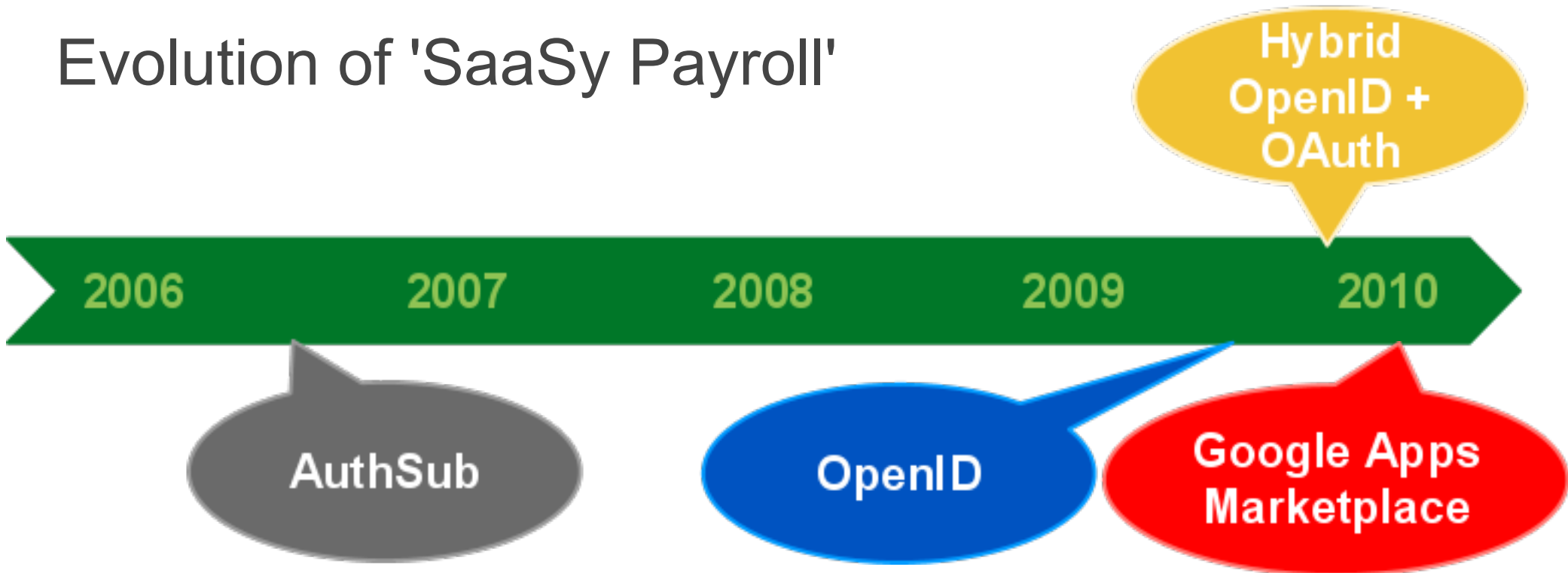
[Sign in as a different user](#)

baayapp.com is asking for some information from your Smart-lawfirm.com account [ryan@smart-lawfirm.com](#)

- Email address: Ryan Boyd (ryan@smart-lawfirm.com)
- Google Calendar

Remember this approval

Evolution of 'SaaSy Payroll'



email	password	openid	token	type	secret
john@foo.com	AxNAAFSnz	-----	ZD1FNKL4	AS	----
jane@goo.com	-----	http://goo.com/1234	JFNB2ANS	----	----
alan@bar.com	----	http://bar.com/6780	D2FNAF7D	3LO	adfa123f
kim@smart-lawfi	----	http://smb.com/123	-----	2LO	----
ryan@smart-law	----	http://smb.com/456	-----	2LO	----
dmb@smart-law	----	http://smb.com/789	-----	2LO	----



[Search accounts](#) [Search Help Center](#)

Thank you for installing SaaSy Payroll. Sign in now to get started. (The application's navigable link may take 24 hours to appear.)

- [Dashboard](#)
- [Users and groups](#)
- [Domain settings](#)
- [Advanced page](#)
- [Support](#)
- [Service settings](#)

SaaSy Payroll settings

App status

✓ Active

✓ Licensed

For pricing and other information, please see the developer's listing.

✓ Enabled

You can temporarily disable this application, preventing users from accessing it without losing any data. [Learn more](#)

[Disable SaaSy Payroll](#)

Data access

✓ Granted

This application is allowed to impersonate the users in your domain and access their data via the following APIs: [Learn more](#)

Calendar (Read/Write, does not require SSL)

This application creates payroll dates on a Google Calendar.

[Revoke data access](#)

Universal navigation

Links

Users in your domain can access this app from Mail, Calendar, Docs, Sites and other Google Apps using the following link in

Google's universal navigation. [Learn more](#)

<http://www.saaasyapp.com/oidlogin.php?fromgoogle&domain=smart-lawfirm.com>

Evolution of 'SaaSy Payroll'

- Improved User Experience
 - Easier on-boarding of users
 - Access granted by appropriate resource owners
- Access to over 2 million businesses
- Multiple code paths

Resources

Resources

- **Google Apps Marketplace:**
<http://developer.googleapps.com/marketplace>
- **Technical docs on Google Apps:**
<http://code.google.com/googleapps/>
- **Technical docs on OpenID and OAuth:**
<http://code.google.com/apis/accounts/>
- **OAuth Playground:**
http://www.googlecodesamples.com/oauth_playground

Q & A

Ask your questions on Google Wave:
<http://bit.ly/magicwave>

Google™

