

# OpenID Single Sign On and OAuth Data Access

## Workshop:

- The Value
- **The Technology**
- The Future

Dave Primmer

Cloud Identity Summit - July 2010

# Agenda

- Terminology
- 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

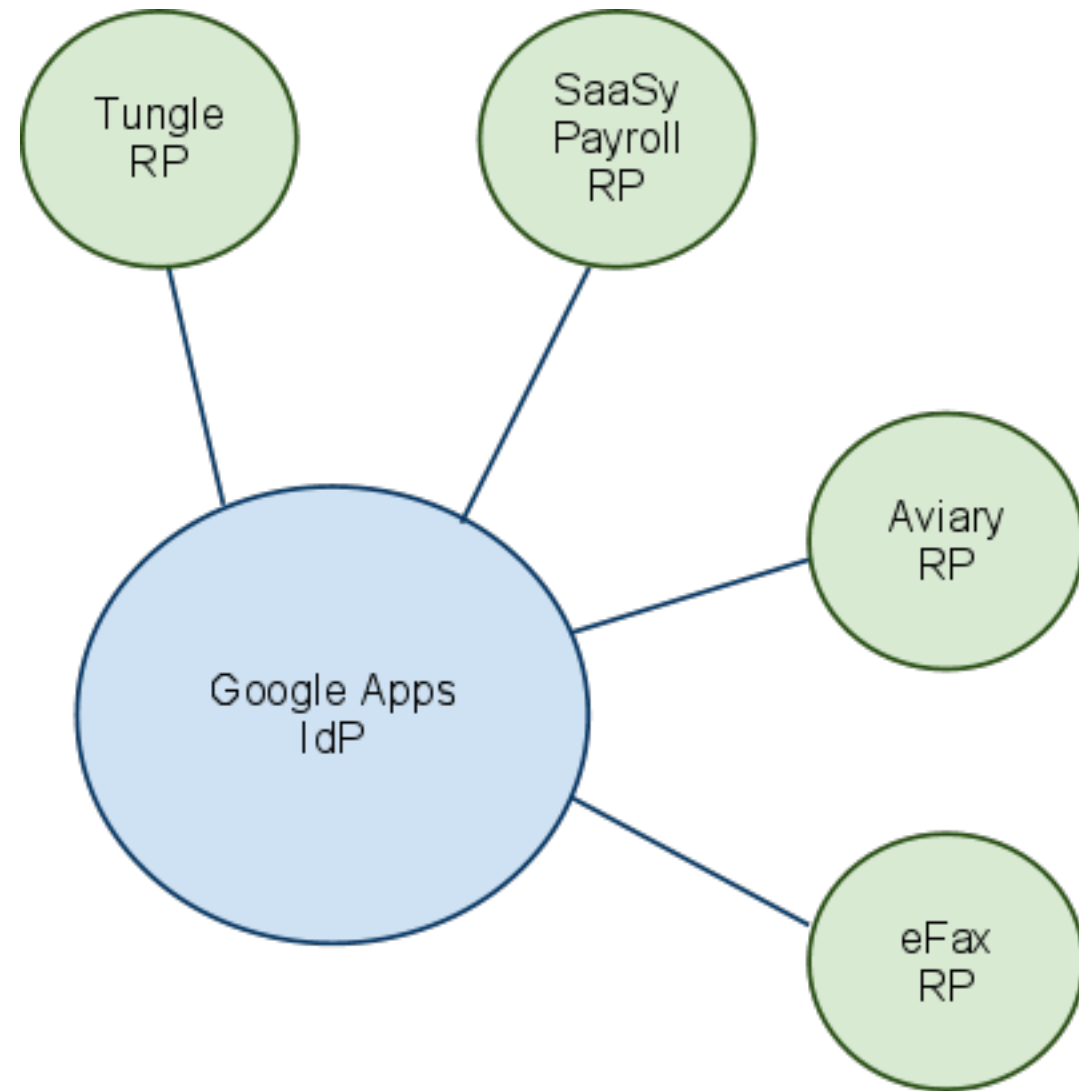
- **Authorization**

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

# 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.

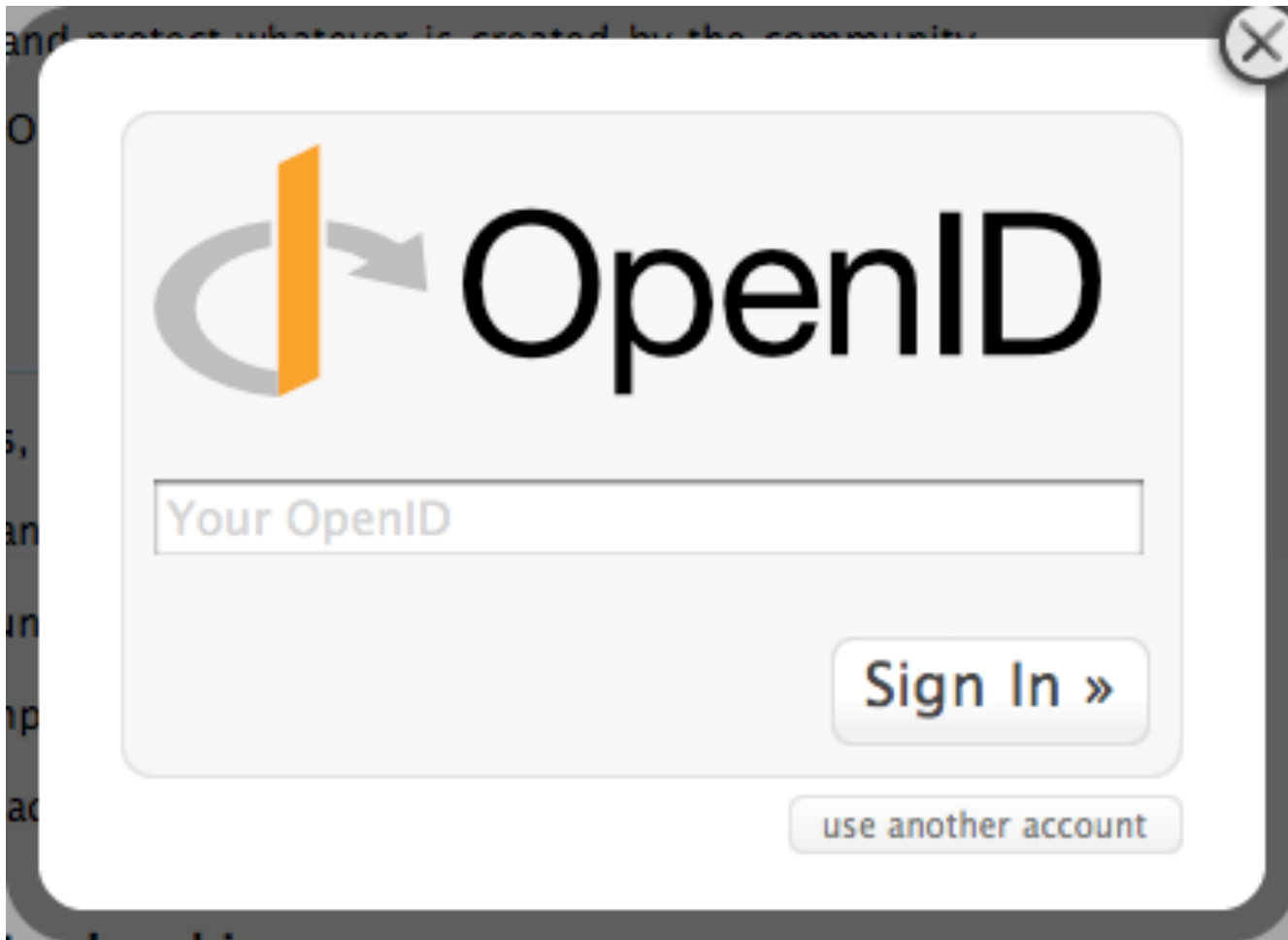




# What information does OpenID provide an app?

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

# OpenID Login Options



and protect whatever is created by the community

O

5,

an

in

op

ac

L. H.

 **OpenID**

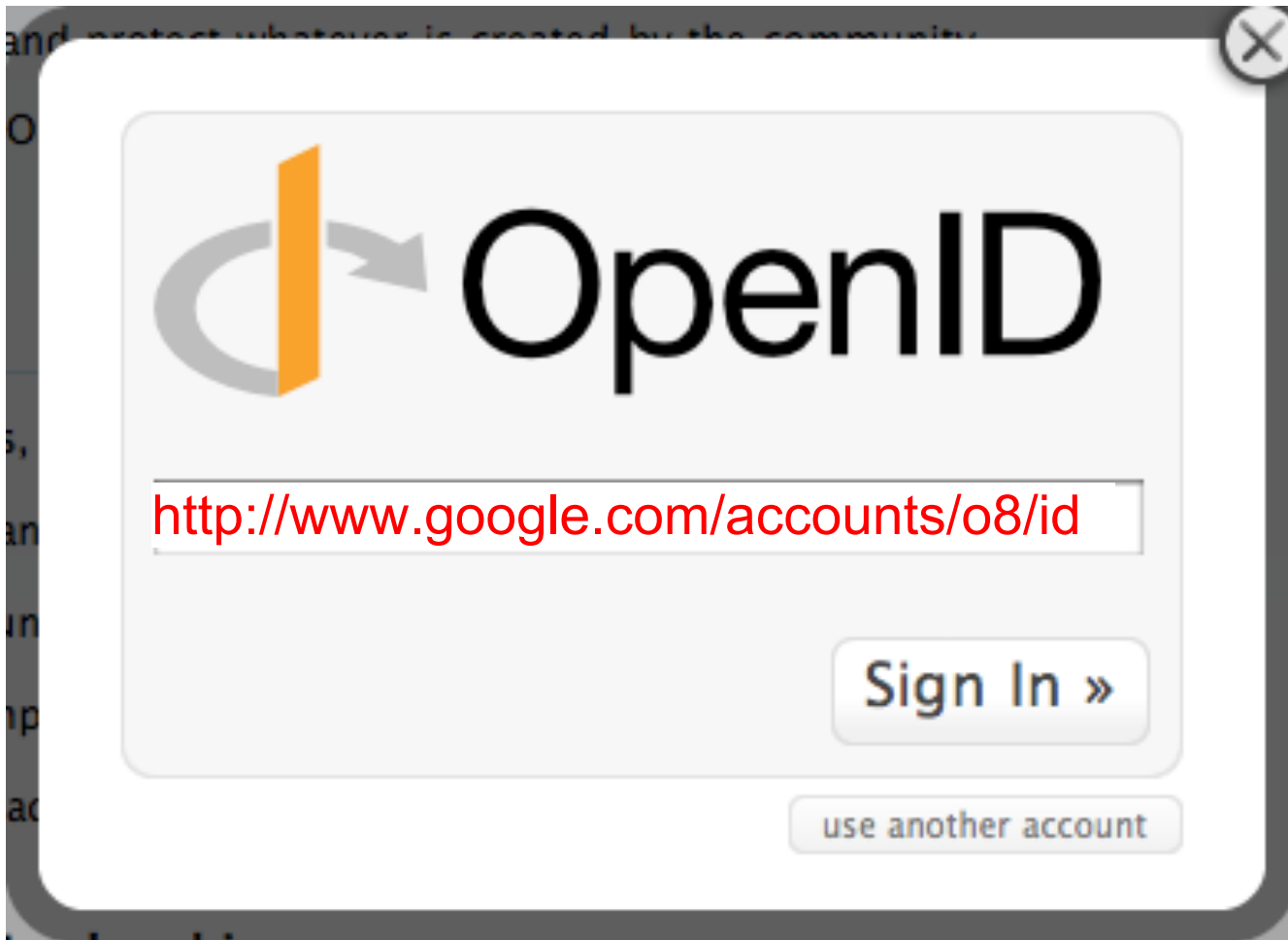
Your OpenID

[Sign In »](#)

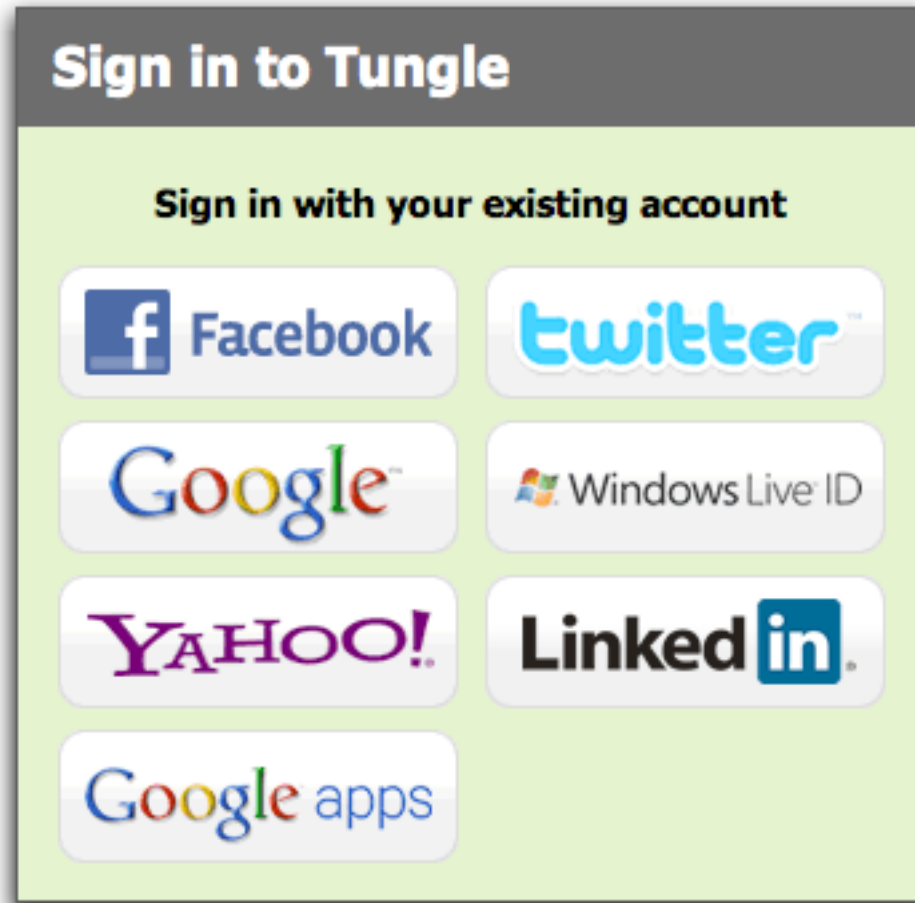
[use another account](#)

The image shows a standard OpenID login dialog box. It features a close button (an 'X' in a circle) in the top right corner. The main content area is light grey and contains the OpenID logo, a text input field with the placeholder text 'Your OpenID', and two buttons: 'Sign In »' and 'use another account'. The dialog box is overlaid on a dark grey background that shows fragments of text from the underlying page.

# OpenID Login Options



# Improved UX



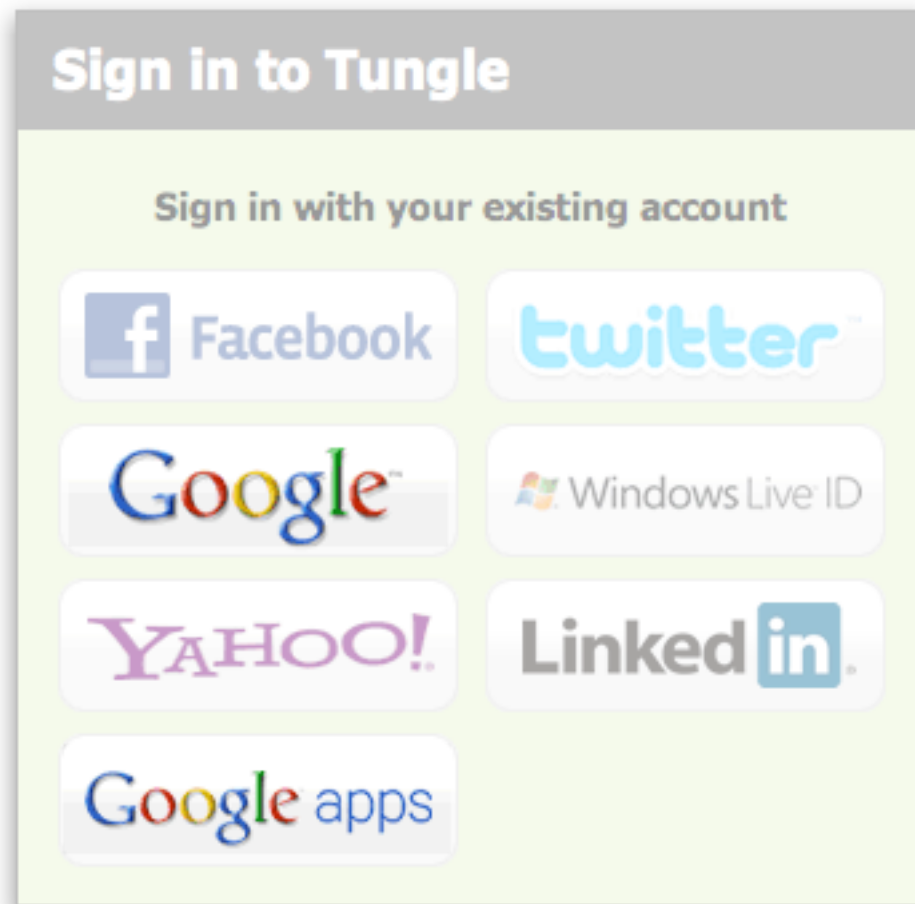
But... what if you want to use an  
OpenID on **your own domain**  
without a complicated URL to  
remember?

# Ideal User Experience: WebFinger

What is your e-mail address?


**Discovery:** Determining the OpenID provider for a user.

# 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>

# Google 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 Libraries

<b>Language</b>	<b>Libraries</b>
<b>Java</b>	OpenID4Java, Step2
<b>.NET</b>	DotNetOpenAuth
<b>PHP</b>	php-openid, php-openid-apps-discovery
<b>Ruby</b>	ruby-openid, ruby-openid-apps-discovery
<b>Any</b>	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



Google calendar

Server

- **Resource Owner**

- owns protected resource
- approves access

**Protected  
Resource**



- **Server**

- receives http request

**Resource  
Owner**

# OAuth Terms

- **Protected Resource**

- resides on server
- requires authorization



**Protected Resource**

- **Resource Owner**

- owns protected resource
- approves access



**Resource Owner**

- **Server**

- receives http request



**Server**



- **Client**

- makes http request



**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 header features the "SaaSy Payroll" logo with the tagline "your payroll solution, your way" and a red "Payroll" button. 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, and a section titled "Future Pay Dates:" lists dates from 5/8/2010 to 5/29/2010. A link to "Add dates to your Google Calendar" is provided at the bottom.

**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/0/0/updateDomain

[ryanboyd@google.com](#) ▾ | [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 **cB7fg1x94QAceEvaCSNYuzP8p**  
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

<p>Three-Legged OAuth</p>		<p>Two-Legged OAuth</p>
<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

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 are search boxes for "Search accounts" and "Search Help Center". A navigation menu contains "Dashboard", "Users and groups", "Domain settings", "Advanced tools" (which is selected), "Support", and "Service settings-". A link "« Back to Advanced tools" 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"/> <a href="#">Learn more about registering new API clients</a>
<b>SaaSy Voice</b>	<b>Docs (Read/Write)</b> https://docs.google.com/feeds/ To export a call log	<input type="button" value="Remove"/>
	<b>Contacts (Read/Write)</b> 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

The screenshot shows the Google Apps Admin console interface. At the top, the browser 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", and the user email `admin@smart-lawfirm.com` circled in red. Below the header is a navigation menu with tabs for "Dashboard", "Users and groups", "Domain settings", "Advanced tools", "Support", and "Service settings-". The main content area is titled "Manage API client access" and contains a form for adding authorized API clients. The form has two input fields: "Client Name" and "One or More API Scopes", both circled in red. Below the "Client Name" field is an example: `www.example.com`. Below the "One or More API Scopes" field is an example: `http://www.google.com/calendar/feeds/ (comma-delimited)`. An "Authorize" button is located to the right of the "One or More API Scopes" field. A red label "Resource Owner" is positioned to the right of the user email. Another red label "Protected Resource" is positioned below the "Authorize" button. 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 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**  **Authorize** [Learn more about registering new API clients](#)

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

**Client** **Docs (Read/Write)** `https://docs.google.com/feeds/`  
To export a call log

**SaaSy Voice** **Contacts (Read/Write)** `https://www.google.com/m8/feeds/` [Remove](#)  
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 smart-lawfirm.com. The browser address bar displays the URL <https://www.google.com/a/cpanel/smart-lawfirm.com/ManageOauthClients>. The user is identified as **admin@smart-lawfirm.com**, labeled as the **Resource Owner**. The navigation menu includes Dashboard, Users and groups, Domain settings, **Advanced tools**, Support, and Service settings. The main heading is **Manage API client access**, with a sub-heading: "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" value="www.saasyapp.com"/> Example: www.example.com	<input type="text" value="http://www.google.com/calendar/feeds/"/> Example: http://www.google.com/calendar/feeds/ (comma-delimited)	<input type="button" value="Authorize"/> <a href="#">Learn more about registering new API clients</a>
<b>Client</b> SaaSy Voice	<b>Docs (Read/Write)</b> https://docs.google.com/feeds/ To export a call log	
	<b>Contacts (Read/Write)</b> https://www.google.com/m8/feeds/ To display names of people who called	<input type="button" value="Remove"/>

At the bottom, 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

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 authorize API clients. Below the instructions, there is a table of authorized API clients. Two entries 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	
<input type="text"/> Example: www.example.com	<input type="text"/> <input type="button" value="Authorize"/> Example: http://www.google.com/calendar/feeds/ (comma-delimited)	<a href="#">Learn more about registering new API client</a>
<b>SaaSy App!</b>	<b>Calendar (Read/Write)</b> https://www.google.com/calendar/feeds/	<a href="#">Remove</a>
	<b>Docs (Read/Write)</b> https://docs.google.com/feeds/ To export a call log	
<b>SaaSy Voice</b>	<b>Contacts (Read/Write)</b> https://www.google.com/m8/feeds/ To display names of people who called	<a href="#">Remove</a>

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 header features the "SaaSy Payroll" logo with the tagline "your payroll solution, your way" and a red "Payroll" button. 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, and a section titled "Future Pay Dates:" lists dates from 5/8/2010 to 5/29/2010. A link to "Add dates to your Google Calendar" is provided at the bottom.

**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

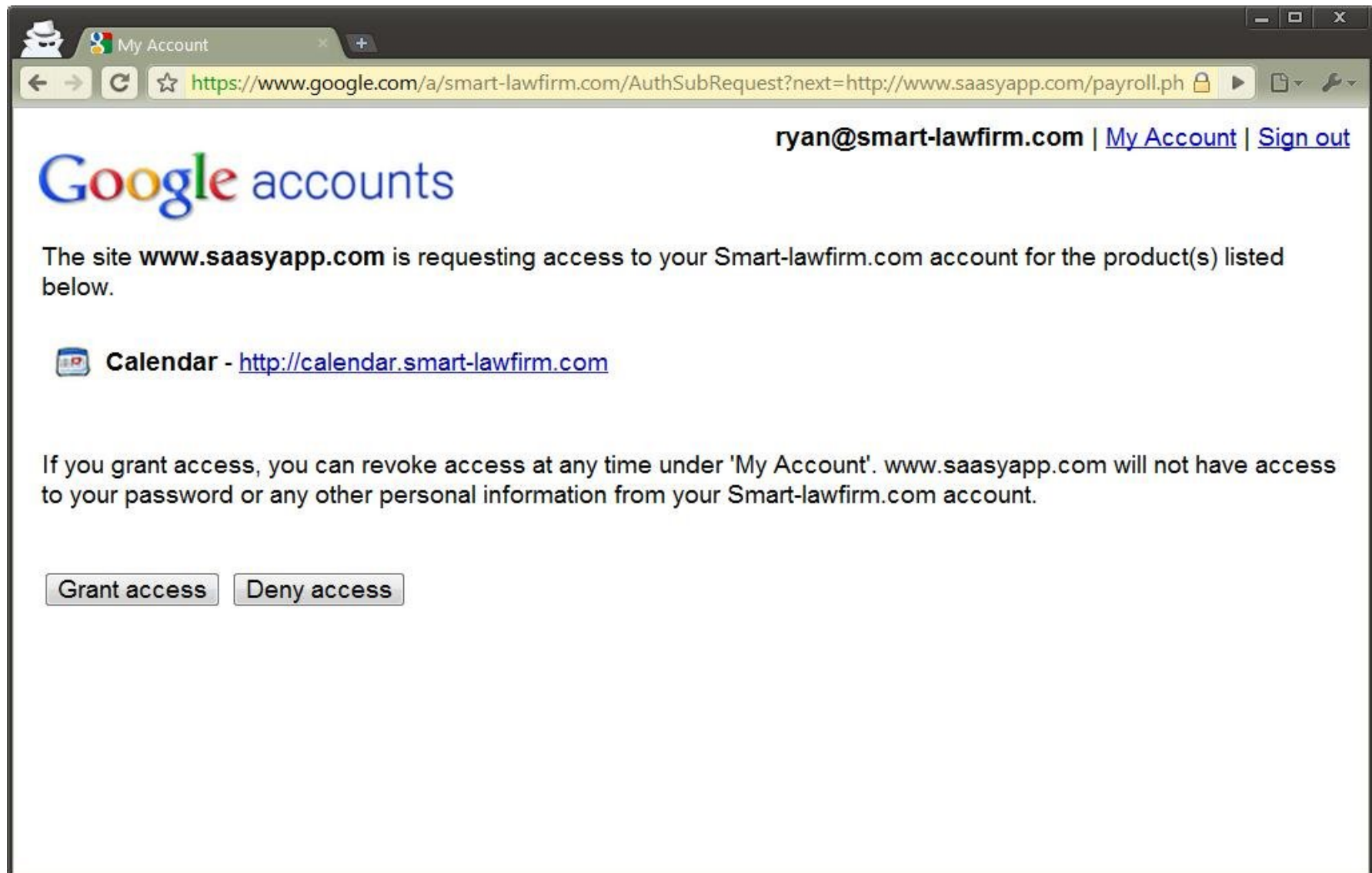
You've worked a lot this week: **74 hours**  
Your hourly rate is: **\$12**

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](#)

# Authorization by Resource Owner



The screenshot shows a 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 title is "My Account". The user is logged in as [ryan@smart-lawfirm.com](mailto:ryan@smart-lawfirm.com) and has links for [My Account](#) and [Sign out](#).

The main heading is "Google accounts". Below it, a message states: "The site **www.saasyapp.com** is requesting access to your Smart-lawfirm.com account for the product(s) listed below."

The requested access is for "Calendar" at the URL <http://calendar.smart-lawfirm.com>.

A disclaimer follows: "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."

At the bottom, there are two buttons: "Grant access" and "Deny access".

# Authorization by Resource Owner

My Account

<https://www.google.com/a/smart-lawfirm.com/AuthSubRequest?next=http://www.saasyapp.com/payroll.ph>

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

**Google accounts**

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

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

**User / Resource Owner**

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.

# 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



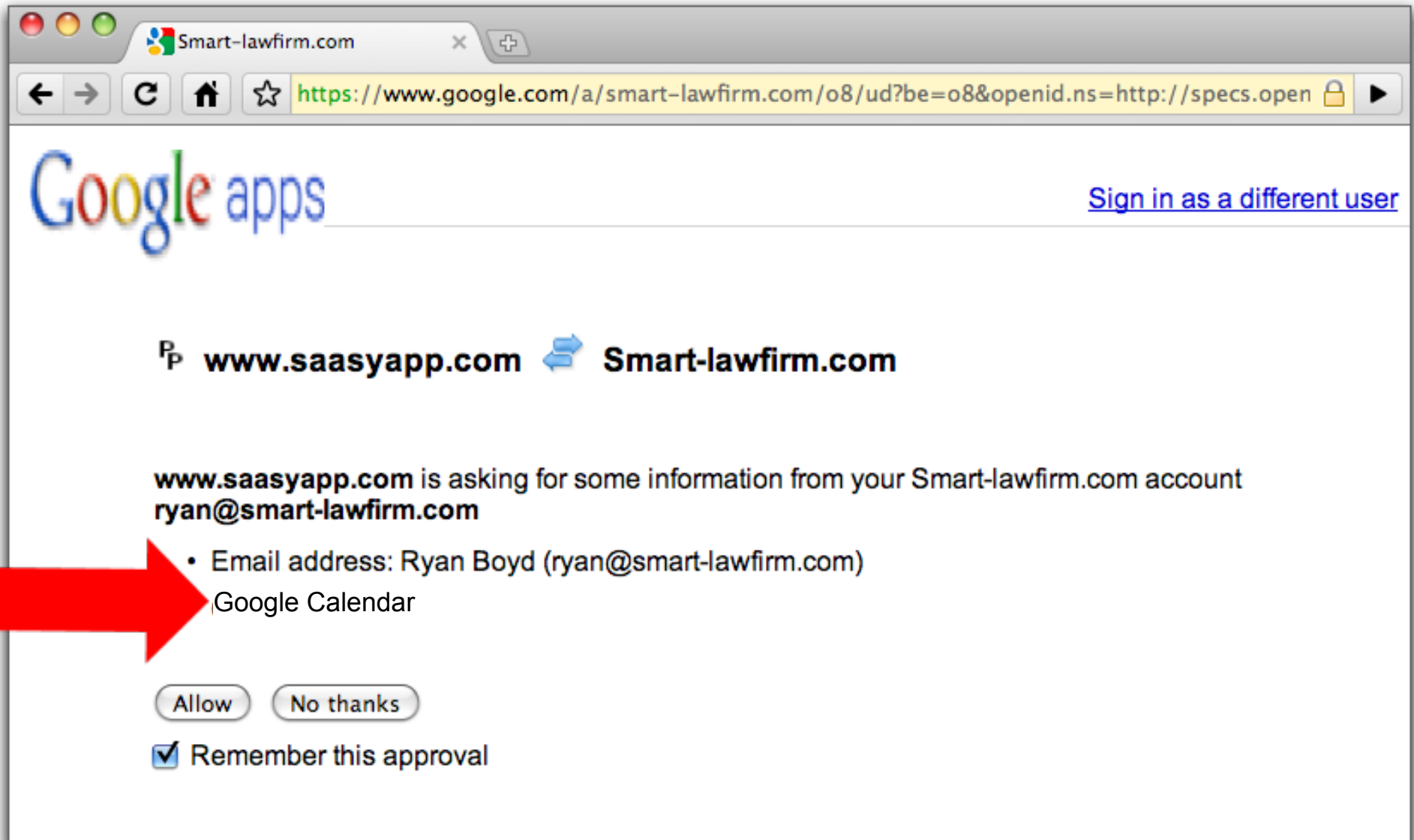
# OAuth 2

- 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

 <a href="#">Print</a>			<a href="#">Day</a>	<a href="#">Week</a>	<b><a href="#">Month</a></b>	<a href="#">4 Days</a>	<a href="#">Agenda</a>
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**  
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**

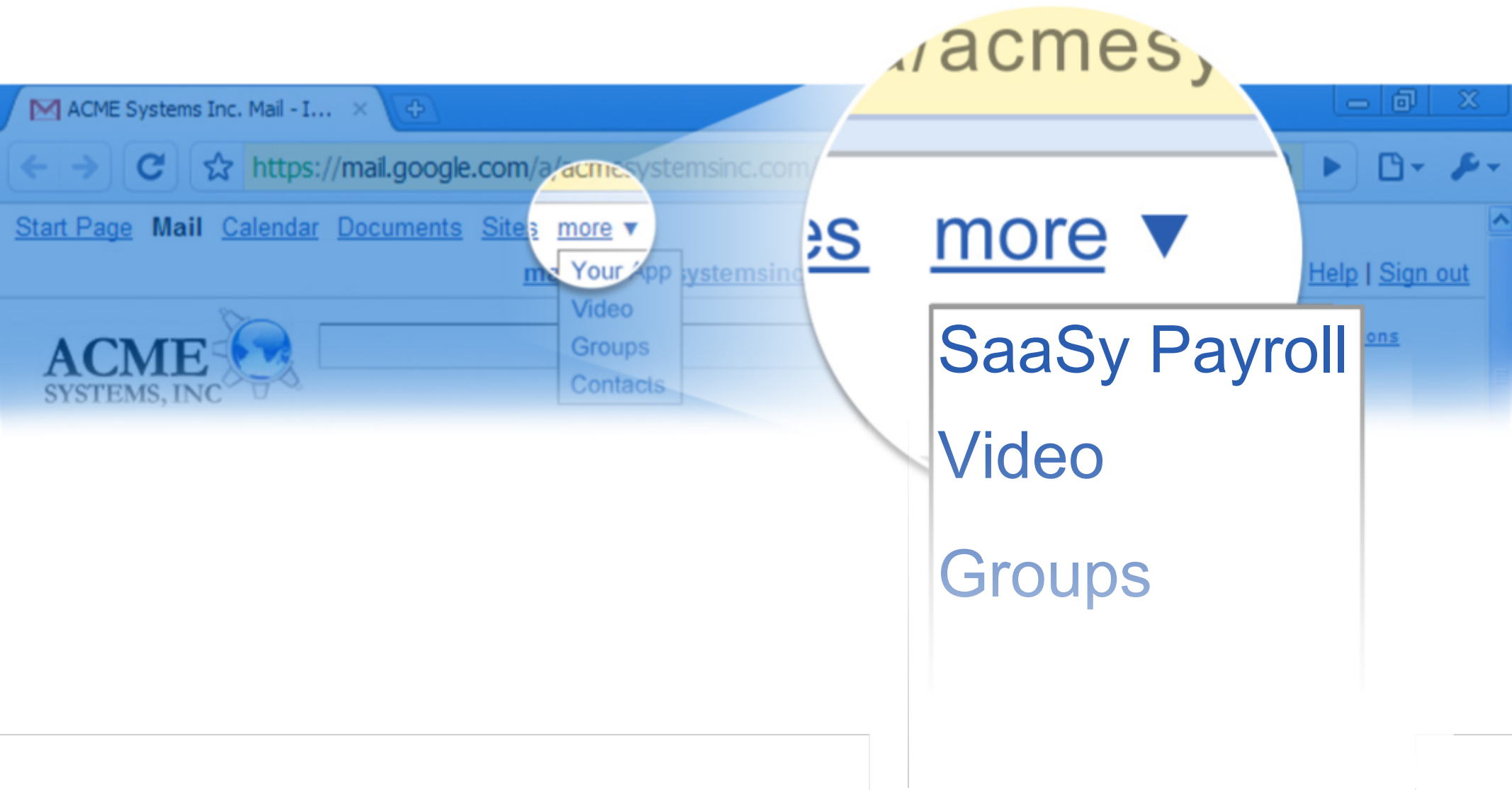
**Data access requirements**

- 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 header features the SaaSy Payroll logo and the tagline "your payroll solution, your way". A red button labeled "Payroll" is visible. The main content area displays the following information:

**Your Paycheck for 5/1/2010**

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

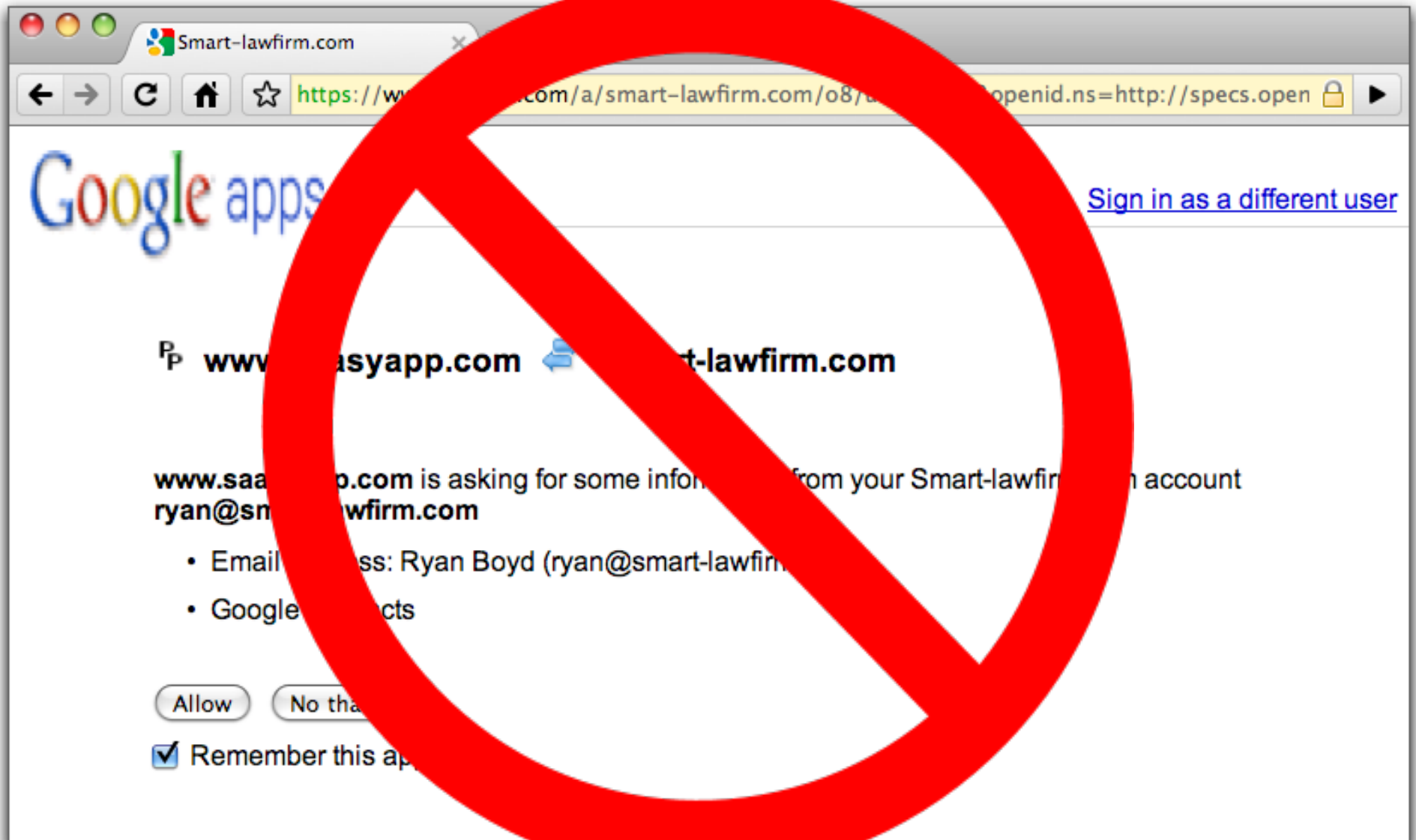
Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

**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 ' SaaS Voice ' service be added to your domain'. Below this, the 'Grant data access' step is highlighted in a sequence of four steps: 1 Agree to terms, 2 Grant data access, 3 External configuration, and 4 Enable the app. A warning message reads: '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.' Three data access permissions are listed with warning icons: '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 'SaaS Voice' includes a link to 'View in the marketplace' and lists features: 'Google universal navigation' and 'Single Sign-On through OpenID'. At the bottom, there are 'Grant data access' and 'Cancel' buttons.

Smart-lawfirm.com x Google Apps x

← → ↻ 🏠 ☆ <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 ' SaaS 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**

SaaS Voice [View in the marketplace](#)

SaaS Voice

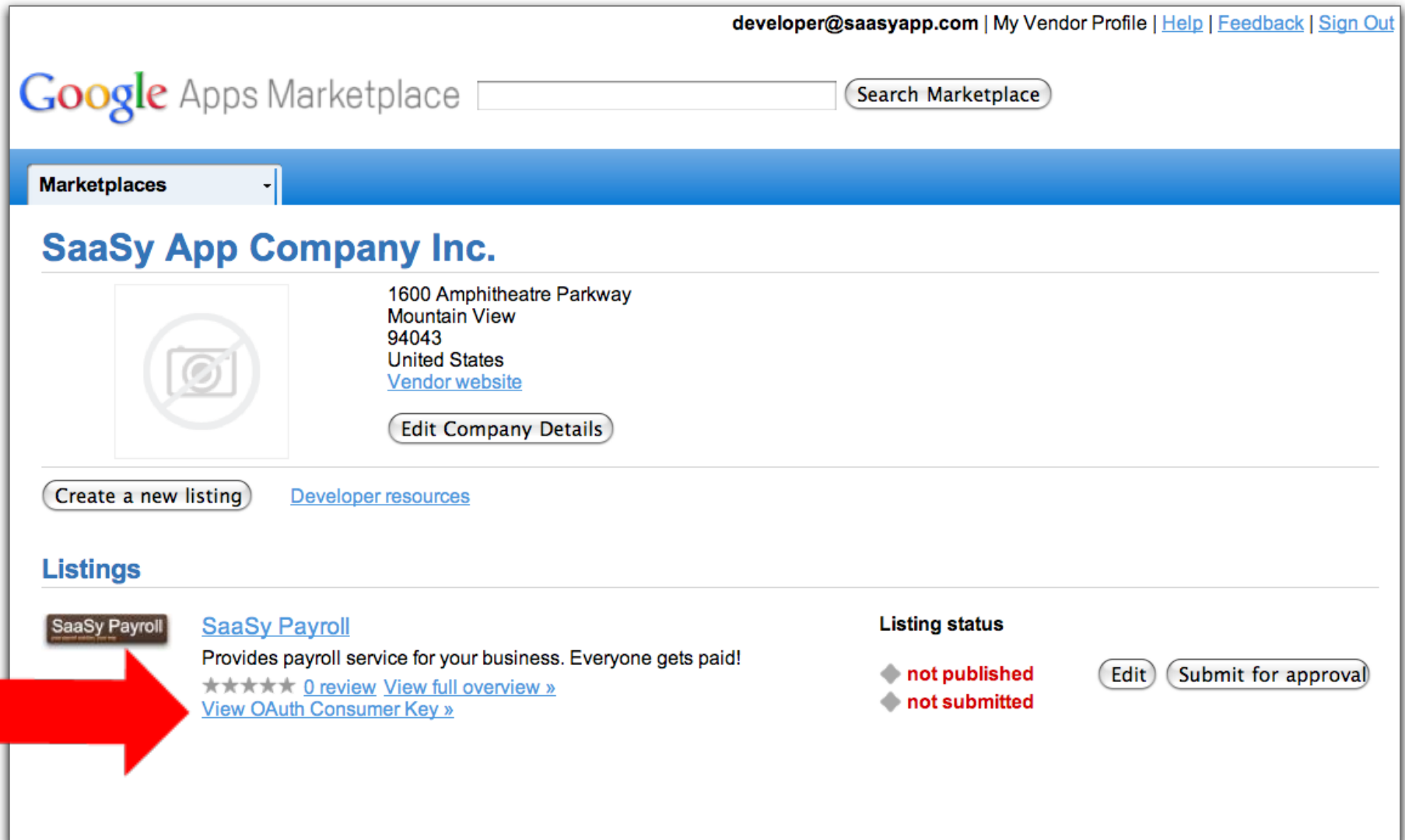
**Includes:**

- 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 ▾

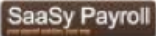
## SaaSy App Company Inc.




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

[Developer resources](#)

### Listings

	<a href="#">SaaSy Payroll</a> Provides payroll service for your business. Everyone gets paid! ★★★★★ <a href="#">0 review</a> <a href="#">View full overview »</a> <a href="#">View OAuth Consumer Key »</a>	<b>Listing status</b> ◆ 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'. A red arrow points to the 'Consumer Key' field. The dialog 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. A warning message 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 of the dialog. Below the dialog, the app listing for 'SaaSy Payroll' is visible, including a description, a 0-star rating, and buttons for 'Edit' and 'Submit for approval'. The status 'not published' and 'not submitted' is shown in red.

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

Google Apps Marketplace  Search Marketplace

Marketplaces

**SaaSy App Company Inc.**  
1600 Amphitheatre Parkway

**Consumer Key / Key Secret: SaaSy Payroll**

Application ID: 907432758210

Consumer Key: 907432758210.apps.googleusercontent.com

Consumer Key Secret: QTE4qgB+THYx8oxbgaP/1/ZG [Regenerate Key Secret](#)

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.

[Close](#)

Provides payroll service for your business. Everyone gets paid!  
★★★★★ [0 review](#) [View full overview >](#)  
[View OAuth Consumer Key >](#)

◆ not published [Edit](#) [Submit for approval](#)  
◆ not submitted

# Summary of Protocols

# Summary of Protocols

<b>3-Legged OAuth</b>	Access data for individual users
<b>2-Legged OAuth</b>	Pre-approved access data for a group of users.
<b>OpenID</b>	Access a user's identity. Can be used for Gmail
<b>OpenID with Google Apps extensions</b>	Access a user's identity for Google Apps accounts
<b>OpenID / OAuth Hybrid</b>	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

<b>email</b>	<b>password</b>
john@foo.com	AxNAAFSnz





# SaaSy Payroll

*your payroll solution, your way*

**Setup**

## New Customer Form

First Name:

Last Name:

E-mail address:

Password:

Confirm Password:

**Signup**

# Evolution of 'SaaSy Payroll'



<b>email</b>	<b>password</b>	<b>token</b>
john@foo.com	AxNAAFSnz	ZD1FNKL4

# Google accounts

The site [www.saasyapp.com](http://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](http://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

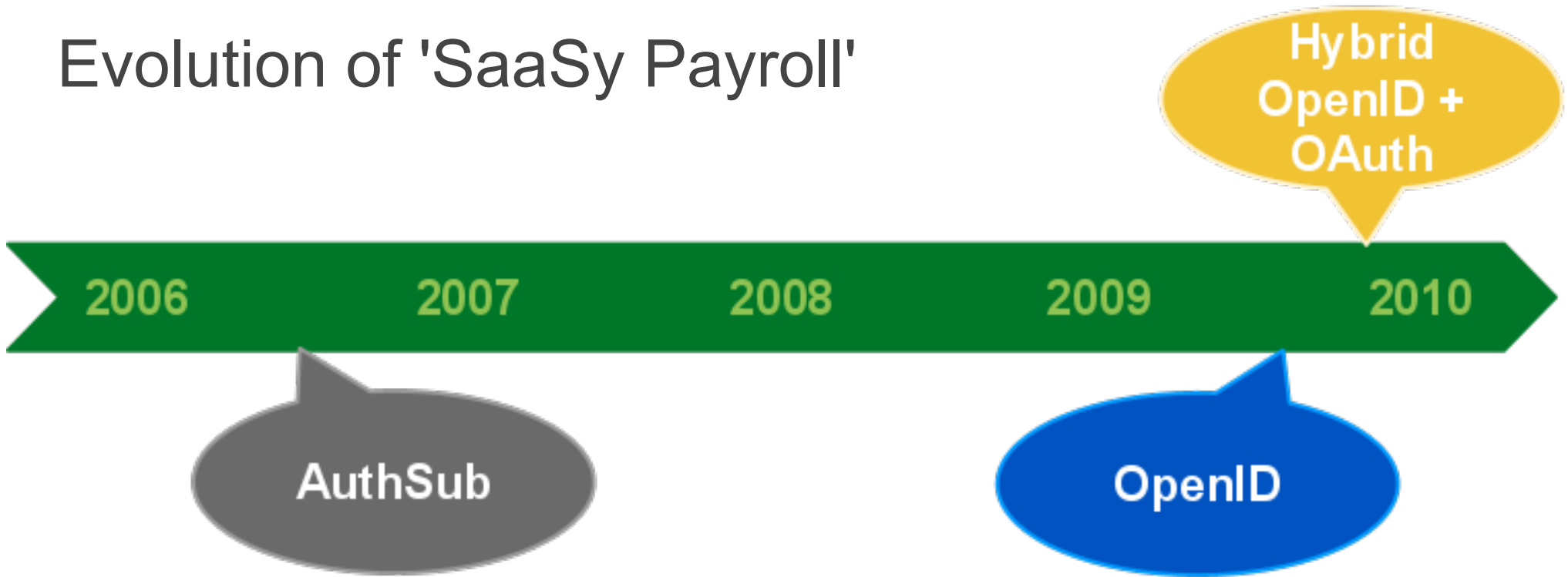
Item	\$
Total wages	888.00
401(k) deduction	(100.00)
Federal income tax	(244.00)
State income tax	(50.00)

### 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



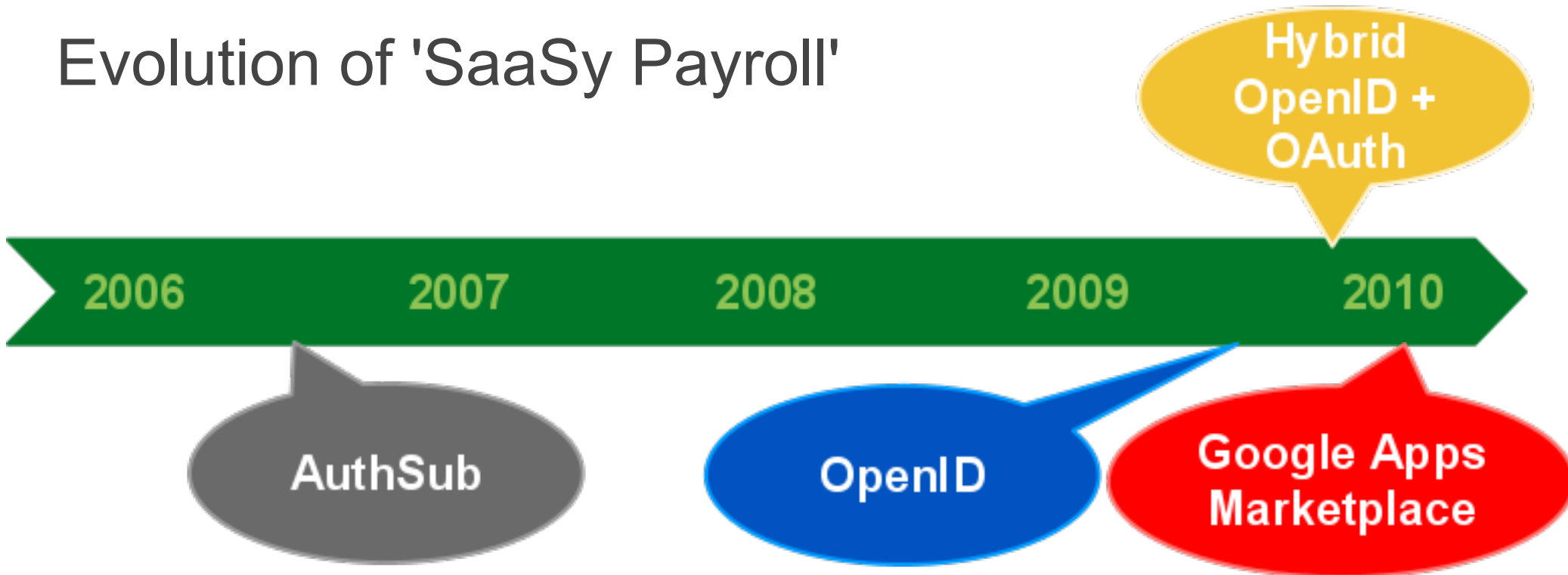
[Sign in as a different user](#)

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](http://www.googlecodesamples.com/oauth_playground)

Q & A