

# Example OAuth Exchange

Service Oriented Architectures Security

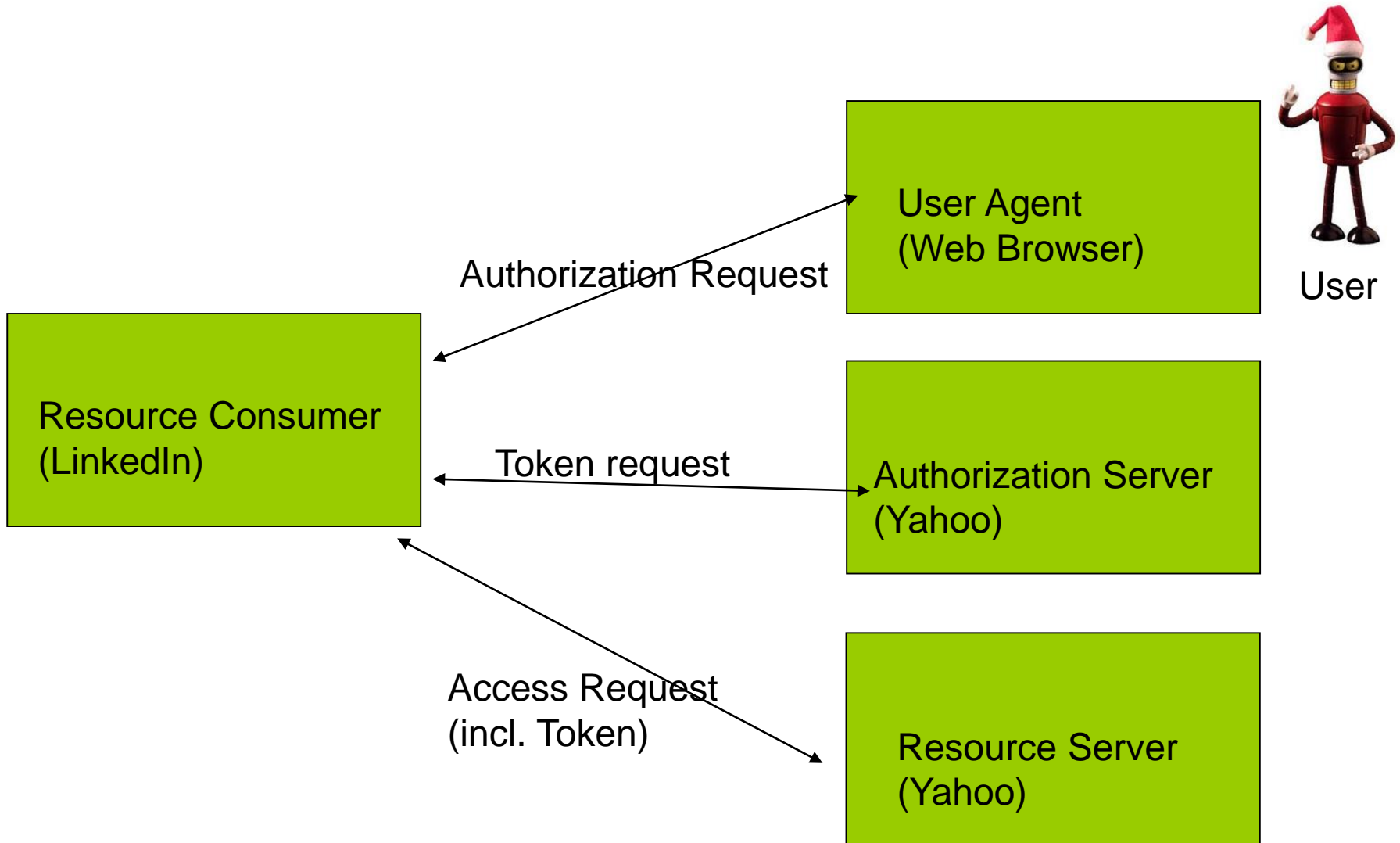
Module 1 - Basic technologies

**Ernesto Damiani**

---

Università di Milano

# Entities






# User navigates to Resource Client



## Build your network *(Why?)* ✕

### Find contacts who are already on LinkedIn

---


 **Web email contacts**  
Check your address book to find contacts who are on LinkedIn.

 Windows Live Hotmail        Gmail       Other

 **YAHOO!**        AOL

[Login to Yahoo!](#)      You will be taken to Yahoo! to enter your username and password.

---

 **Address book contacts** [Find](#)  
Outlook, Apple Mail, etc.

# User authenticated by Authorization Server

**Sign in to Yahoo!**

To start using this service...

- Step 1: Sign in to Yahoo!**  
Yahoo! encourages folks with new ideas to work with Yahoo!'s own tools and services to make them even better and more useful for you. You'll need to sign in to allow them to work with the personal information that you keep with Yahoo!.
- Step 2: Give your permission.**  
After you sign in we'll ask you to give us permission to share your personal data with the developer of this service.

**Sign in to Yahoo!**

**Are you protected?**  
Create your sign-in seal. (Why?)

Yahoo! ID:  
  
(e.g. free2rhyme@yahoo.com)

Password:

**Keep me signed in**  
for 2 weeks unless I sign out. [Info](#)  
[Uncheck if on a shared computer]

[Forget your ID or password?](#) | [Help](#)

**Don't have a Yahoo! ID?**  
Signing up is easy. [Sign Up](#)

**One Yahoo! ID. So much fun!**  
Use it to check mail, listen to music, share photos, play games, instant

# User authorizes Resource Consumer to access Resource Server

Yahoo! - Terms - Microsoft Internet Explorer provided by NOKIA

File Edit View Favorites Tools Help

Address [https://api.login.yahoo.com/W5Login/V1/wslogin?appid=cVa\\_PAFIkY2KjGtd2IKZeJTUNp8fLBX4KmA&ts=1215323357&sig=a1401bd223c0127d681911983863a6338&scrumb=hmM0aryi.3I](https://api.login.yahoo.com/W5Login/V1/wslogin?appid=cVa_PAFIkY2KjGtd2IKZeJTUNp8fLBX4KmA&ts=1215323357&sig=a1401bd223c0127d681911983863a6338&scrumb=hmM0aryi.3I) Go Links SnagIt

Yahoo! - Help

## YAHOO!

### Now we need your permission to grant access to your Yahoo! account

<http://www.linkedin.com> is asking you and Yahoo! for the ability to automatically log you into your Yahoo! account through a service or application that is provided by <http://www.linkedin.com>, and to:

- read your data in **Yahoo! Address Book**
- read and write to your data in **Yahoo! Address Book**

By clicking "I Agree" below, you give Yahoo! permission to enable <http://www.linkedin.com> to access your Yahoo! account for this purpose, and further agree to the Automatic Login Terms of Service below.

Keep in mind:

- <http://www.linkedin.com> will not be able to access any data you keep on Yahoo! other than the data identified above.
- The permission will expire in 2 weeks.
- You can change this permission by visiting the [My Account](#) page and selecting the **Partner Accounts** link. Note that revoking permission may take up to 24 hours.
- If you change your password, you may be required to give permission again.
- The Yahoo! privacy policy does not apply to <http://www.linkedin.com>; please read their privacy policy to learn more about how they treat your personal information.
- Yahoo! has no affiliation with <http://www.linkedin.com> and cannot guarantee the security of any user data that you permit <http://www.linkedin.com> to access.

#### Sign-in Permissions

Please review the following terms and indicate your agreement below. [View all and print](#)

Automatic Login Terms of Service - Please read carefully

Your use of automatic login with third party sites is at your sole risk. While Yahoo! takes measures to protect the privacy and

By clicking "I agree", you agree that you have read and understand these terms.

# Resource Client calls the Resource Server API

LinkedIn: Imported Contacts: Newly Added Contacts - Microsoft Internet Explorer provided by NOKIA

File Edit View Favorites Tools Help

Address http://www.linkedin.com/uploadContacts?checkUpload=&handle=%2Fp%2F2%2F000%2F00c%2F1ba%2F2F4701f%2Etxt&taskType=importContacts&refreshCount=1&context=5&sortAction=lastname Go Links SnagIt

Account & Settings | Help | Sign Out

People | Jobs | Answers | Companies Advanced Search People Search

We added 20 contact(s).

Home Groups Profile Contacts Inbox Add Connections

Chandra Kiran Architect at Nokia India Pvt Ltd Your profile is 25% complete [ Edit ]

**Contacts** Connections Imported Contacts Network Statistics Add Connections Remove Connections

These are your newly added contacts that are not yet connected to you on LinkedIn. Invite them to connect!

Select All Showing 20 of 20 contacts.

**A**  **A, Razool** ahmdrasool@yahoo... See details >

**B**  **Babu, Sudheer** vsnair2@yahoo.com See details >

**C**  **C P, Mahir** cpmahir@yahoo.co... See details >

**C, Hari** hchembukave@ya... See details >

**G**  **goel, amit** Architect at SemanticInsights amitgoelamit@gmail... See details >

**K**  **K, Ranjith** ...

Razool, A  
Sudheer, Babu  
Mahir, C P  
Hari, C  
amit, goel  
Ranjith, K  
Sajil, Koroth  
Amitava, Kundu  
Rghunathan, Navaneethan  
Ram, P N

Add a personal note to your invitation

Invite selected contacts

# Remark: Authentication

**Yahoo in our example may be outside the authentication part to other providers (e.g. using OpenID).**

**Authorization Server and Resource Server do**



# Remark: Authorization

**Asking the user for consent prior to share information is considered privacy-friendly.**

**User interfaces for obtaining user content may not always be great.**

Google accounts



Launchpad.37signals.com is asking for some information from your Google Account [hannes.tschofenig@gmail.com](mailto:hannes.tschofenig@gmail.com)

- Google profile: [hannes.tschofenig](#)

Remember me



# Remark: Authorization, cont.

VeriSign, Inc. (US) <https://pip.verisignlabs.com/authenticate?target=render&identityName=hannestschofenig>

test Headlines Apple Yahoo! Google Maps YouTube Wikipedia News Popular Apple Yahoo! Google

RFC 3929 http:...txt IETF Jul... htt...htm REST A... smartp... Cliqset ...

VeriSign Labs  
**Personal Identity Portal** Beta

**Sign In with Your OpenID**

Personal Icon

The Web site, <http://www.tschofenig.priv.at/wp/> is requesting verification that **hannestschofenig** is your OpenID.

Select when you want the trust relationship for this site to expire and click **Allow** to verify your identity.

Click **Deny** to deny this request and return to <http://www.tschofenig.priv.at/wp/>.

**Trusted Site Expiration**

Expiration	<input checked="" type="radio"/> Never Expire
	<input type="radio"/> Expire on: Nov 10 2010
	<input type="radio"/> Expire After Signing In

**Deny** **Allow**

# Remark: Authorization, cont.

Trusted Sites					
Date ▲	Web Address ▼	OpenID ▼	Transaction Type ▼ ?	Expiration ▼	Action
2010-11-10	https://launchpad.37	hannestschofenig	Authentication	Never	<a href="#">Edit</a>   <a href="#">Delete</a>
2010-11-09	https://launchpad.37	hannestschofenig	Authentication	2010-11-10	<a href="#">Edit</a>   <a href="#">Delete</a>
2009-05-13	https://my.pbworks.c	hannestschofenig	Data Exchange	Never	<a href="#">Edit</a>   <a href="#">Delete</a>
2008-12-20	http://my.pbwiki.com	hannestschofenig	Data Exchange	Never	<a href="#">Edit</a>   <a href="#">Delete</a>
2008-08-13	http://emailtoid.net/	hannestschofenig	Data Exchange	Never	<a href="#">Edit</a>   <a href="#">Delete</a>

Trusted Site Expiration	
<b>Nickname</b>	HannesTschofenig
<b>Email</b>	Hannes.Tschofenig@gmx.net
<b>Fullname</b>	Hannes Tschofenig
<b>Expiration</b>	<input checked="" type="radio"/> Never Expire <input type="radio"/> Expire on: <input type="text" value="Month"/> <input type="text" value="Day"/> <input type="text" value="Year"/> <input type="radio"/> Expire Immediately

Cancel

Save

# Remark: Authorization, cont.

## Request for permission

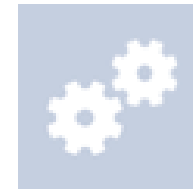
---

OAuth 2.0 Test is requesting permission to do the following:



### Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.



OAuth 2.0 Test

[Report application](#)

Logged in as Hannes Tschofenig (Not you?)

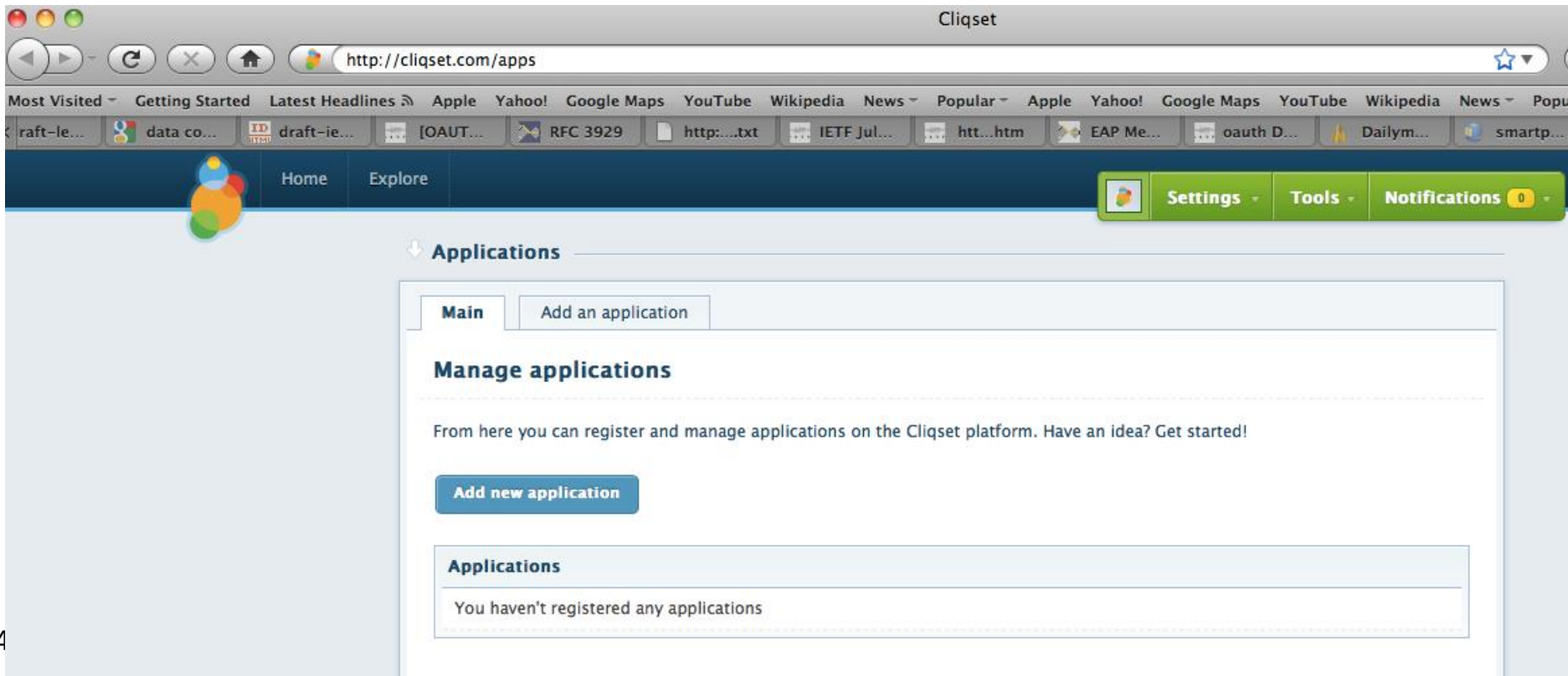
Allow

Don't allow

# Remark: Prior-Registration

Many Resource Server require registration of Resource Client's prior to usage.

Example: <http://developer.cliqset.com/api>



The screenshot shows a web browser window titled "Cliqset" with the address bar displaying "http://cliqset.com/apps". The browser's address bar and tabs are visible, along with a navigation menu containing "Home" and "Explore". On the right side of the navigation bar, there are buttons for "Settings", "Tools", and "Notifications" (with a "0" indicator). The main content area is titled "Applications" and features a "Main" tab and an "Add an application" button. Below this, the heading "Manage applications" is followed by the text: "From here you can register and manage applications on the Cliqset platform. Have an idea? Get started!". A prominent blue button labeled "Add new application" is displayed. At the bottom, a section titled "Applications" contains the message: "You haven't registered any applications".

# Remark, cont.

## Application details

Application name:

Description:

A brief description of your application. Keep it under 500 characters.

Logo:

Browse...

JPEG, GIF, or PNG up to 500kb; it will be resized to 150x50

Icon:

Browse...

JPEG, GIF, or PNG up to 500kb; it will be resized to 16x16

Website URL:

The home page of your company or organization.

Callback URL:

Where should we return to after successfully authentication?

Create application

Cancel

# History

# History

**November 2006:** Blaine Cook was looking into the possibility of using OpenID to accomplish the functionality for delegated authentication. He got in touch with some other folks that had a similar need.

**December 2006:** Blaine wrote a "reference implementation" for Twitter based on all the existing OAuth-patterned APIs, which Blaine and Kellan Elliott-McCrea turned into a rough functional draft

**April 2007:** [Google group](#) was created with a small group of implementers to write a proposal for an open protocol.

**July 2007:** OAuth 1.0 (with code for major programming languages)

**September 2007:** Re-write of specification to focus on a single flow (instead of "web", "mobile", and "desktop" flows)

**Deployment of OAuth well on it's way:**  
<http://wiki.oauth.net/ServiceProviders>

# History, cont.

## **1<sup>st</sup> OAuth BOF (Minneapolis, November 2008, IETF#73)**

- BOF Chairs: Sam Hartman, Mark Nottingham
- BOF went OK but a couple of charter questions couldn't be resolved.

## **2<sup>nd</sup> OAuth BOF (San Francisco, March 2009, IETF#74)**

- BOF Chairs: Hannes Tschofenig, Blaine Cook
- Charter discussed on the mailing list and also during the meeting. Finalized shortly after the meeting

## **IETF wide review of the OAuth charter text (28<sup>th</sup> April 2009)**

- Announcement: <http://www.ietf.org/mail-archive/web/ietf-announce/current/msg06009.html>

## **OAuth working group was created (May 2009)**

- Chairs: Blaine Cook, Peter Saint Andre

## **Feb 2010: 'The OAuth 1.0 Protocol' approved as Informational RFC:**

- <http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07047.html>



# History, cont.

**March 2010: Peter Saint Andre became Area Director and Hannes Tschofenig became Blaine's co-chair.**

**March 2010: IETF OAuth meeting in Anaheim**

**April 2010: OAuth 2.0 <[draft-ietf-oauth-v2-00.txt](#)> published co-authored by Eran, Dick, David.**

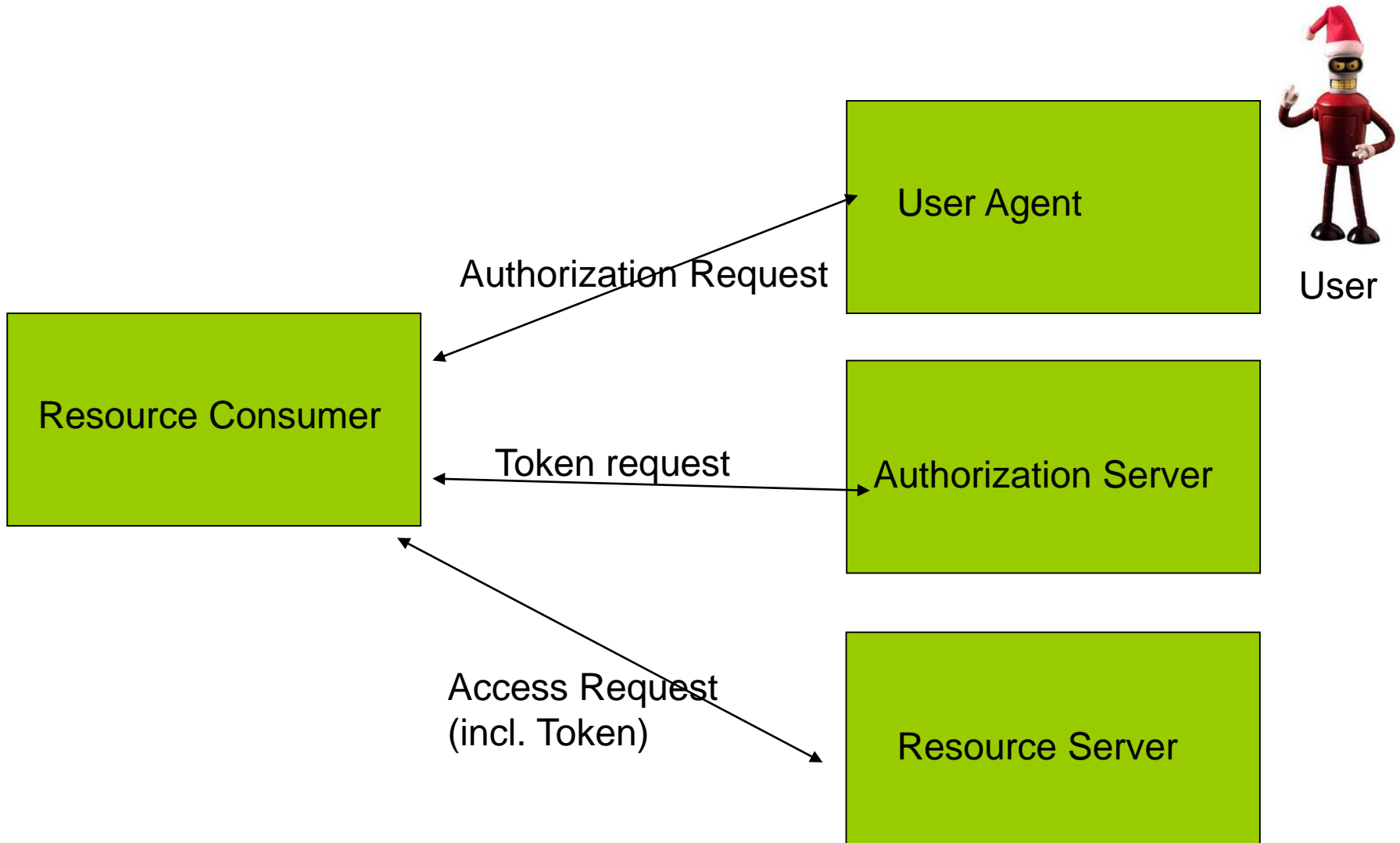
**May 2010: First OAuth interim meeting co-located with IIW to discuss open issues.**

**July 2010: Maastricht IETF meeting**

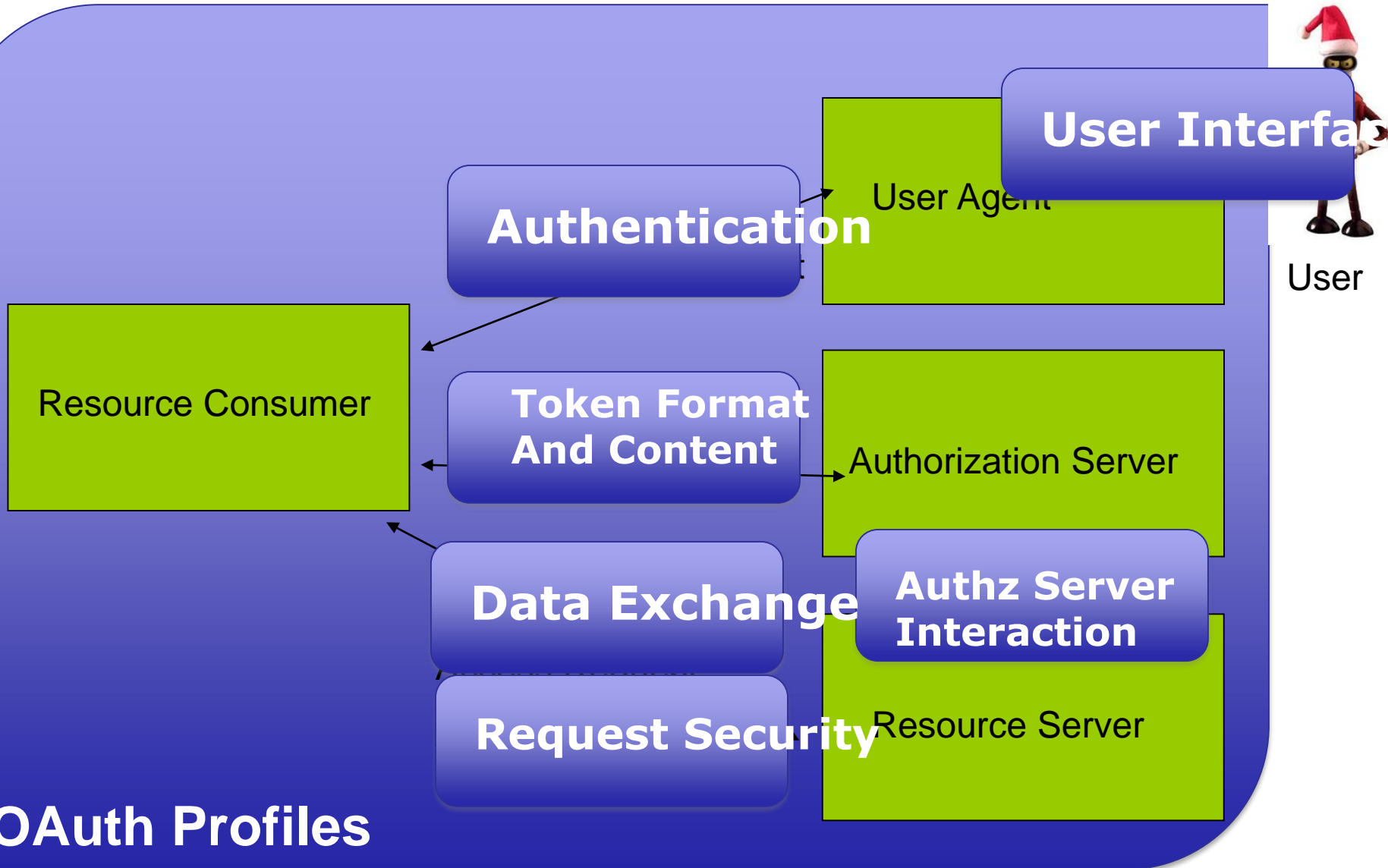
**November 2010: Document split into "abstract" specification and separate bearer token and message signing specification.**

**November 2010: Beijing IETF meeting – no official OAuth working group meeting. Discussions about security for OAuth**

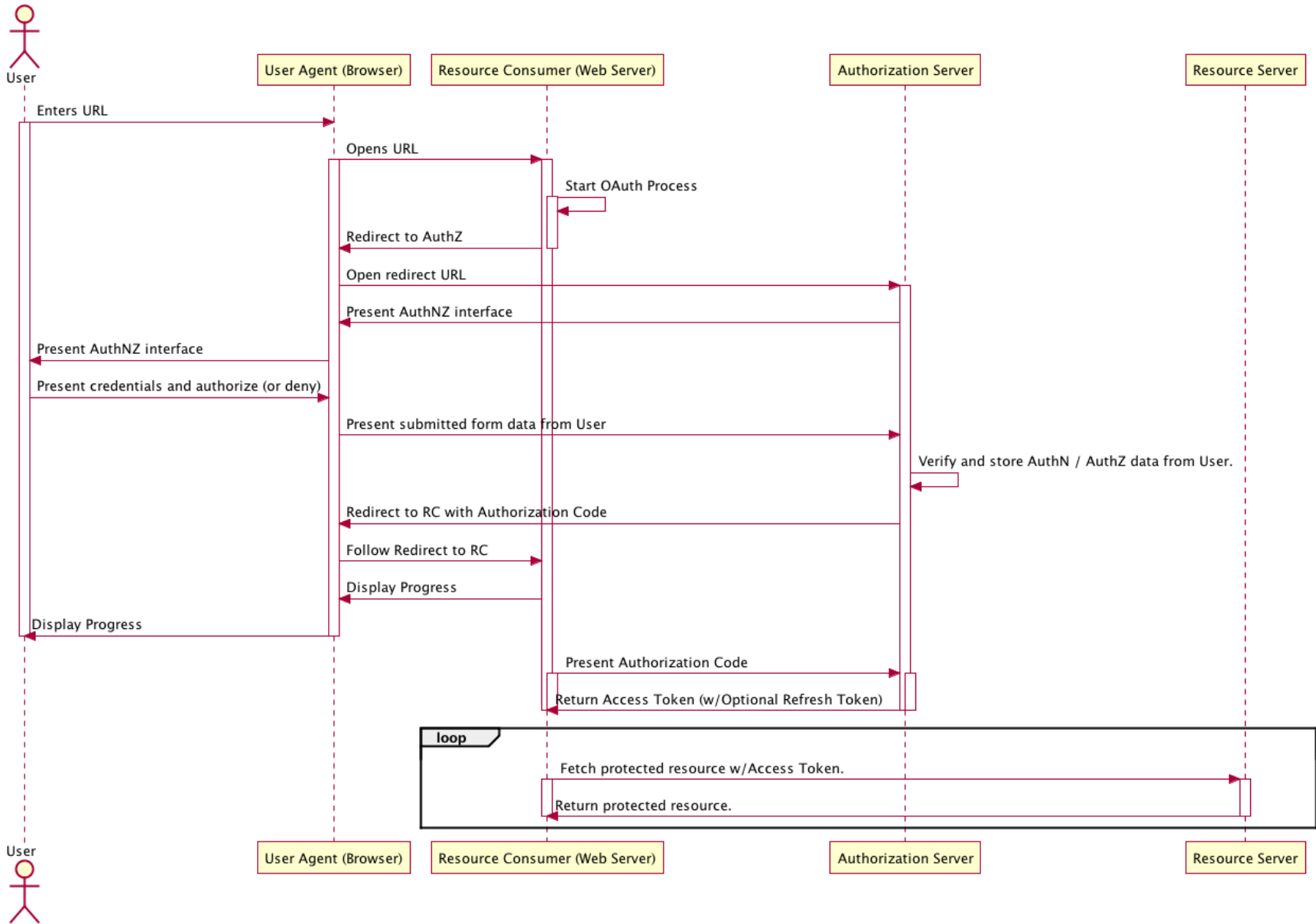
# Entities



# Work Areas



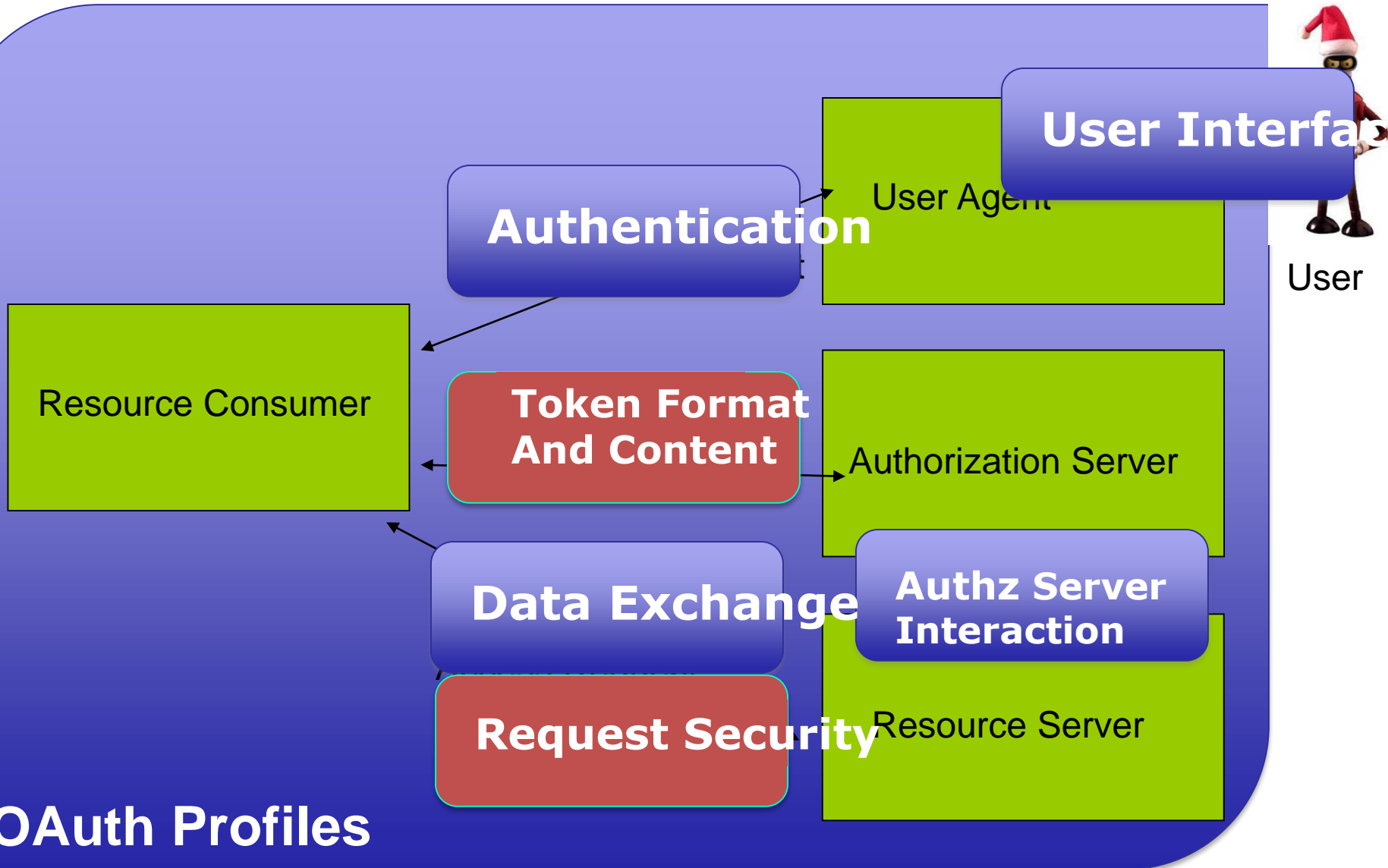
# **Web Server Flow**



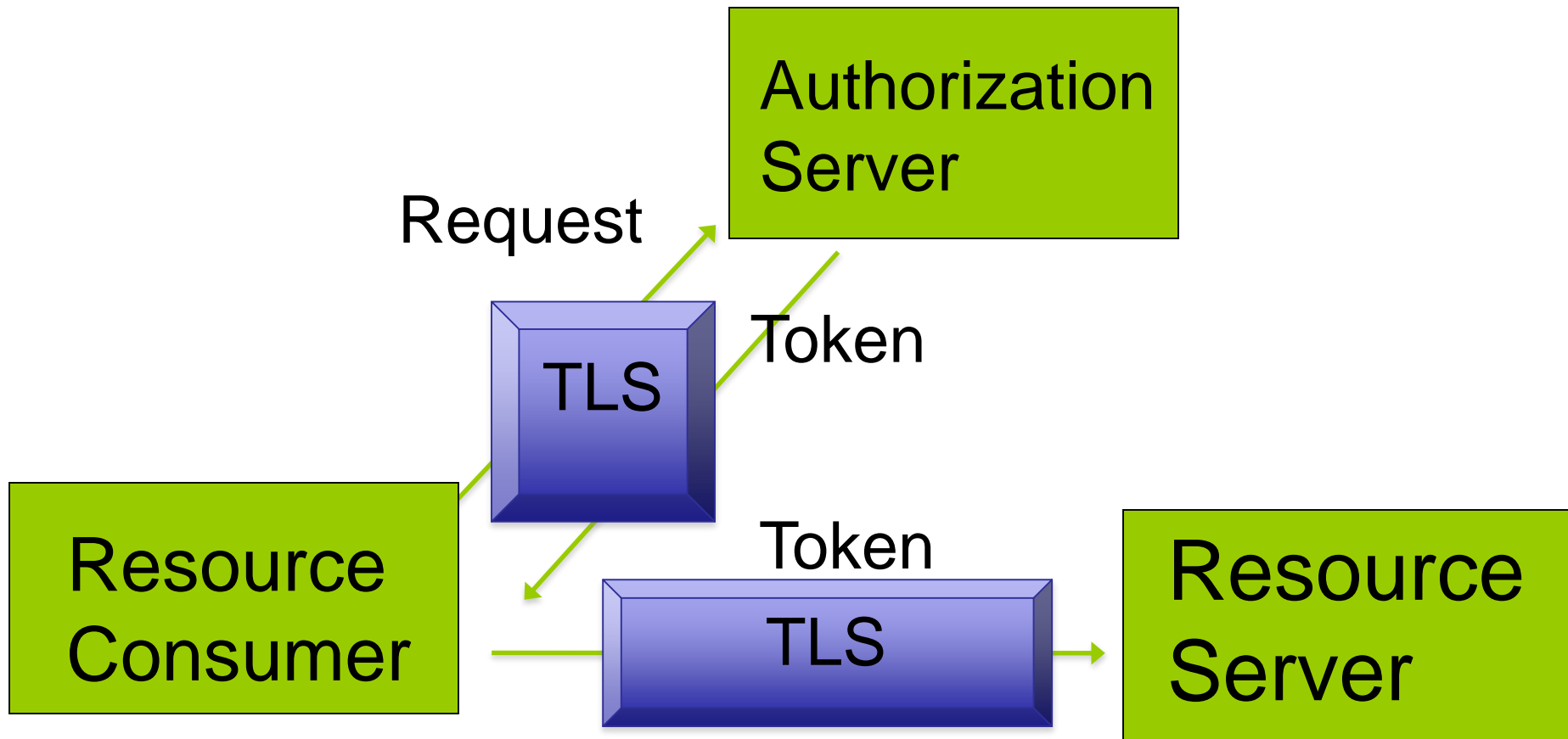
**A little bit about OAuth security...**



# Work Areas

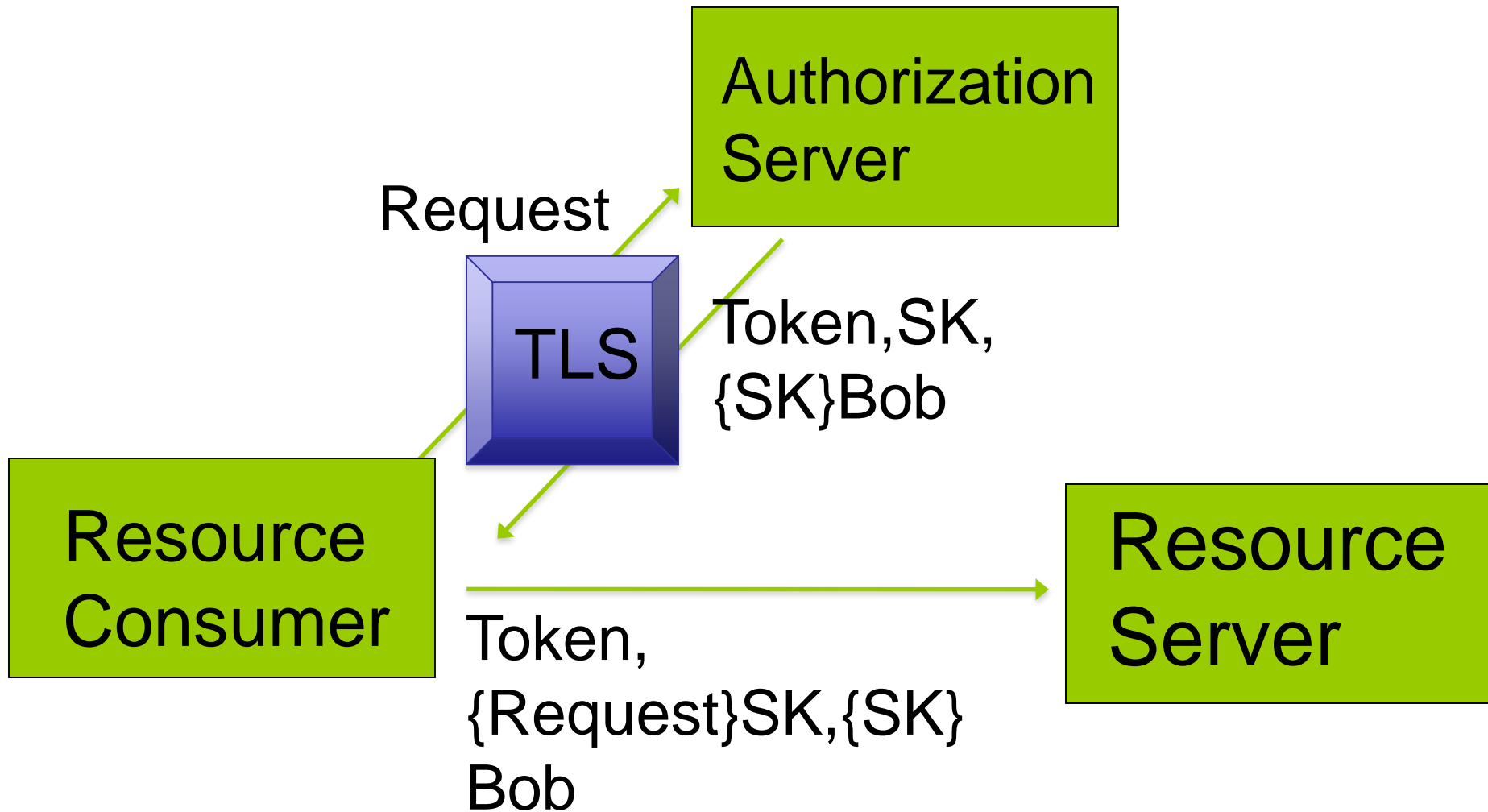


# “Bearer Token”





# “Message Signing”



## Conclusion

**Open Web Authentication (OAuth) is developed in the IETF to provide delegated authentication for Web-based environments.**

- Usage for non-Web based applications has been proposed as well.

**Join the OAuth mailing list at**

**<http://datatracker.ietf.org/wg/oauth/charter>**