

local.ch<sup>+</sup>



# OpenID

Open Distributed Identity Management

Cédric Hüsler

Webtuesday Zürich - January 2007

# Quick Poll

Who always use the same PW for every new account on a new site?

Who has an OpenID?

Who has a Google Account?

prove you are really who you suppose to be

# Authentication

Username & Password

Challenge-response

Public-Private Key

vs.

what are you allowed to do

# Authorization

ACL (Access Control List)

RBAC (Role-based Access Control)

ability to uniquely identify yourself

# Identity

Your Name

AHV-Nr / SSN

Fingerprint

vs.

ability to control what others know about you

# Privacy

can you keep a secret?

Virtualization

Opt-in

how much can I depend on you?

trust

vs.

control

how much information am I going to give?

# SSO

Single-Sign-On



using the same  
credentials to access  
multiple services



automatic  
authentication beyond  
session and service



Authentication

Identity

SSO

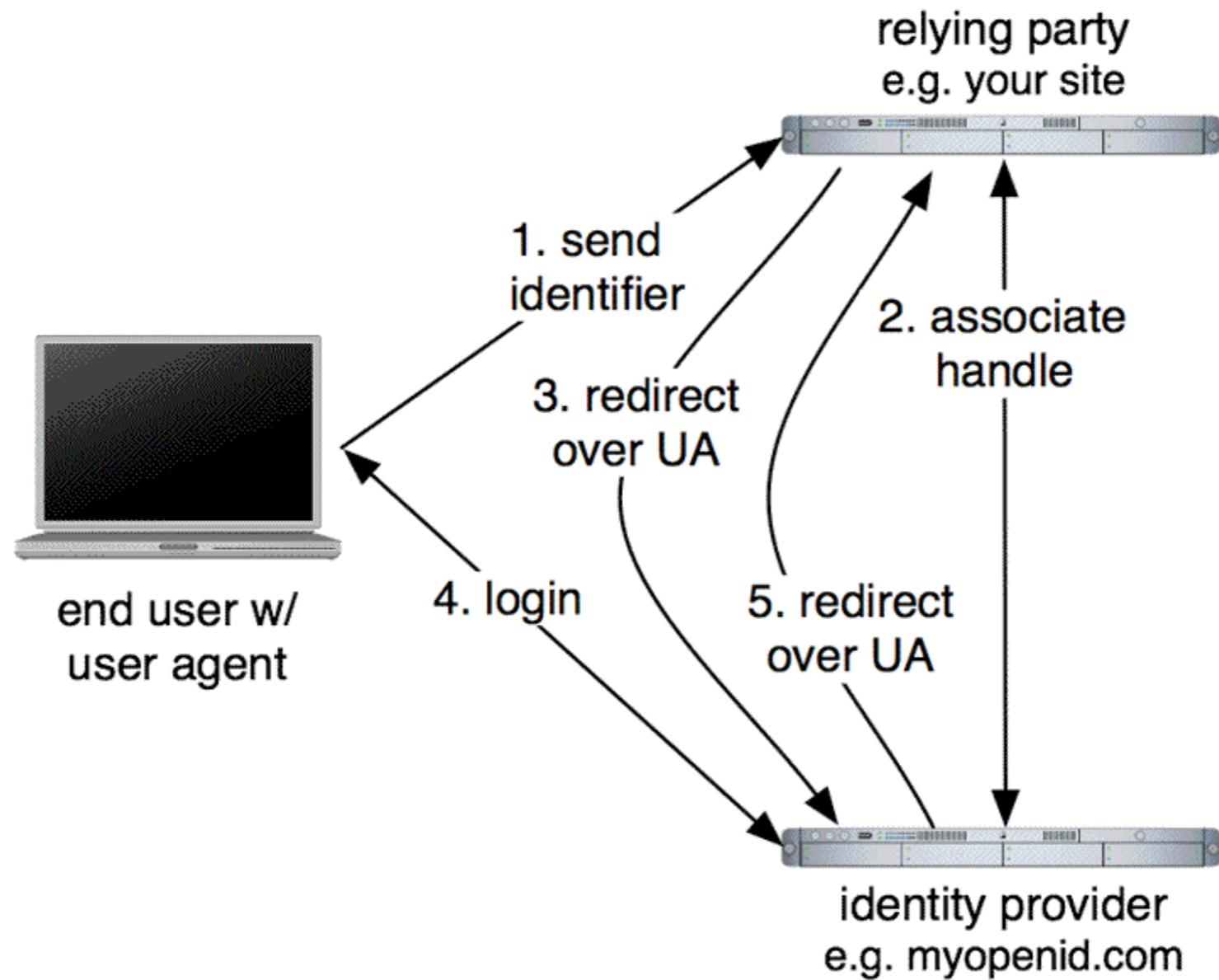
# Use a URI\* as Username!

I own keepthebyte.ch

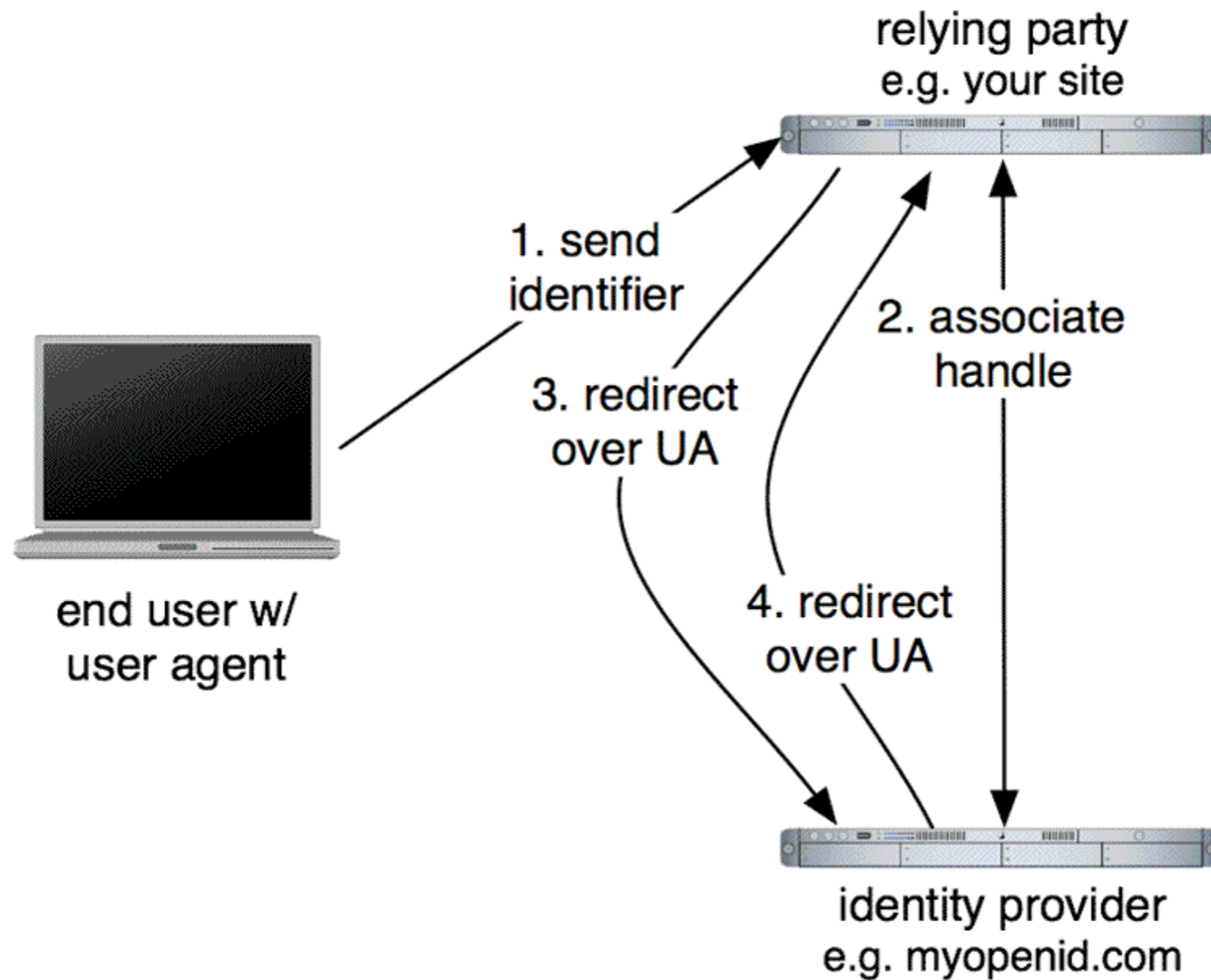
- why not using it as my global username?

Time for a demo...

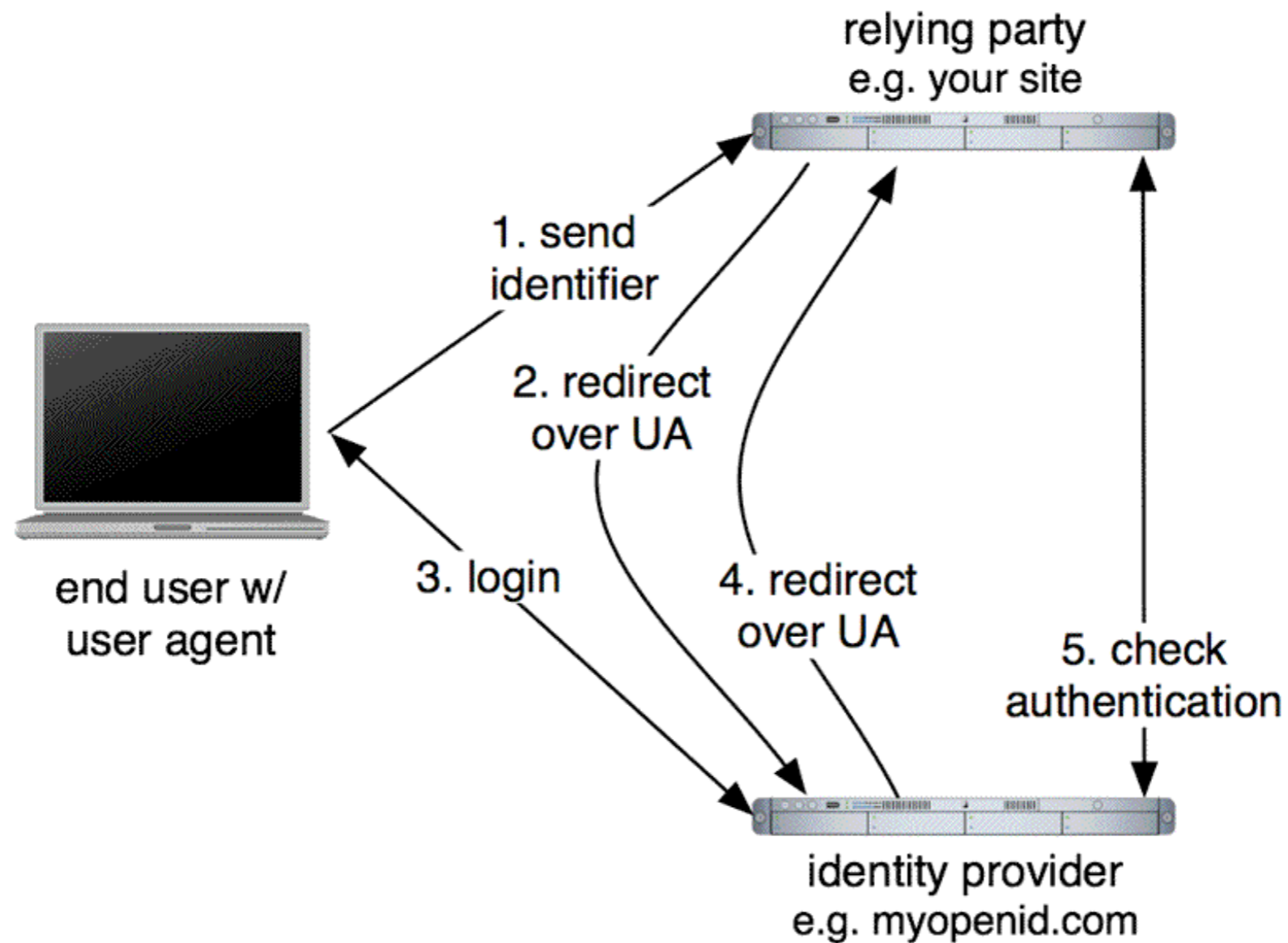
# Process Overview



# ...with Auto Login

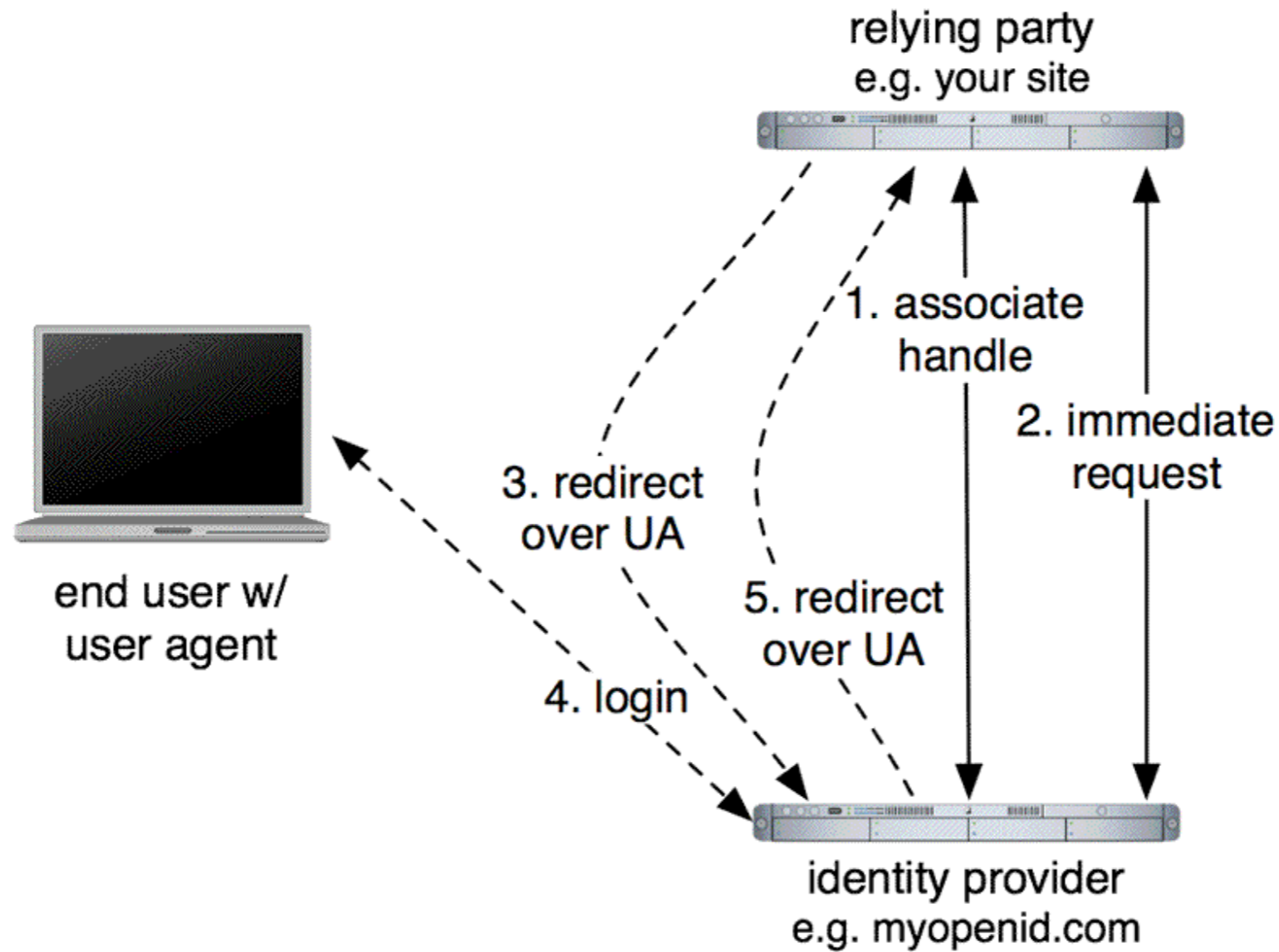


# ...Stateless (Dump Mode)



Not recommended due Security Issue!

# ... Instant (Immediate Mode)



# Delegated Authentication

My OpenID:

keepthebyte.myopenid.com

Add these lines to the root HTML document of the domain “keepthebyte.ch”:

```
<link rel="openid.server" href="http://www.myopenid.com/server" />  
<link rel="openid.delegate" href="http://keepthebyte.myopenid.com" />  
<meta http-equiv="X-XRDS-Location" content="http://keepthebyte.myopenid.com/xrds" />
```

Now I can use this as my OpenID:

keepthebyte.ch

# Properties Exchange

Manage personal profile information centrally on the OpenID Provider site

Maybe even have multiple Persona - like MyOpenID is offering

Define what profile properties are allowed to be share with the site you like to login

A screenshot of a web form for editing a persona profile. The form is titled "Persona Name" and has a dropdown menu set to "Default". Below this are two checkboxes: "Make this my default persona" (checked) and "Make this my public persona" (unchecked). A horizontal line separates this section from the main profile fields. The fields include: "Nickname" (text input: keepthebyte), "Full Name" (text input: Cédric Hüsler), "E-mail Address" (text input: myopenid@keepthebyte.com), "Birth Date" (three dropdown menus for Month, Day, and Year), "Postal Code" (text input), "Gender" (dropdown menu: ---), "Country" (dropdown menu: Switzerland), "Time Zone" (dropdown menu: Europe/Zurich), and "Preferred Language" (dropdown menu: English).

A screenshot of a web page showing a summary of the profile. The title is "Default" and there is an "edit" link in the top right corner. The profile information is listed as follows: "Nickname keepthebyte", "Full Name Cédric Hüsler", "E-mail Address myopenid@keepthebyte.com", "Country CH", "Time Zone Europe/Zurich", and "Preferred Language EN". At the bottom of the page, there are three buttons: "Allow Forever", "Allow Once", and "Deny".

# Implementation



LIVEJOURNAL



## OpenID Providers

- [MyOpenID.com](http://MyOpenID.com), [VeriSign PIP](http://VeriSign PIP), ...
- List: [openid.net/wiki/index.php/Public\\_OpenID\\_providers](http://openid.net/wiki/index.php/Public_OpenID_providers)

## Specification

- [openid.net](http://openid.net)

## List of Libraries & Enabled Software

- [openid.net/wiki/index.php/Libraries](http://openid.net/wiki/index.php/Libraries)

# And You?

1 Create your own OpenID

2 Make your blog/site OpenID ready!

A good starting point is to allow users to sign comments and leave ratings with OpenID

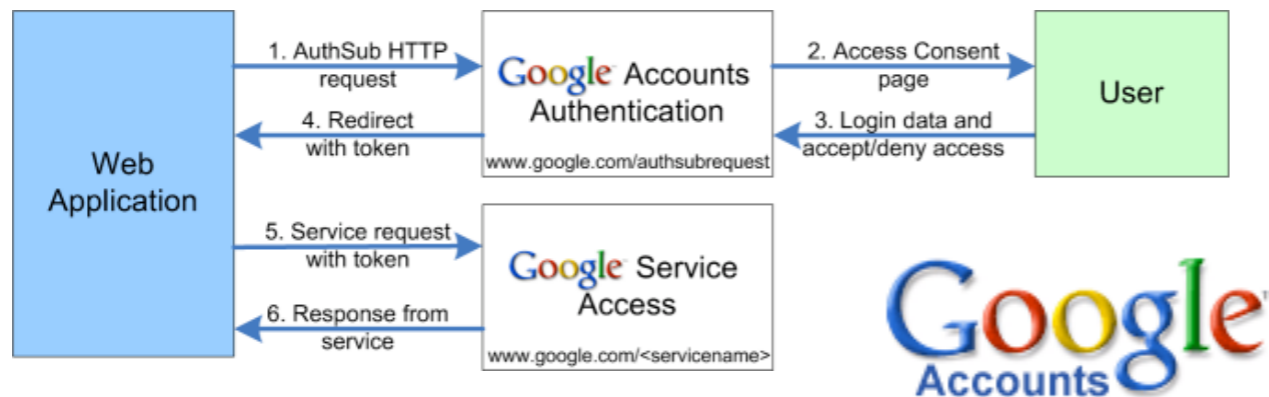
4 Show friends how it works...



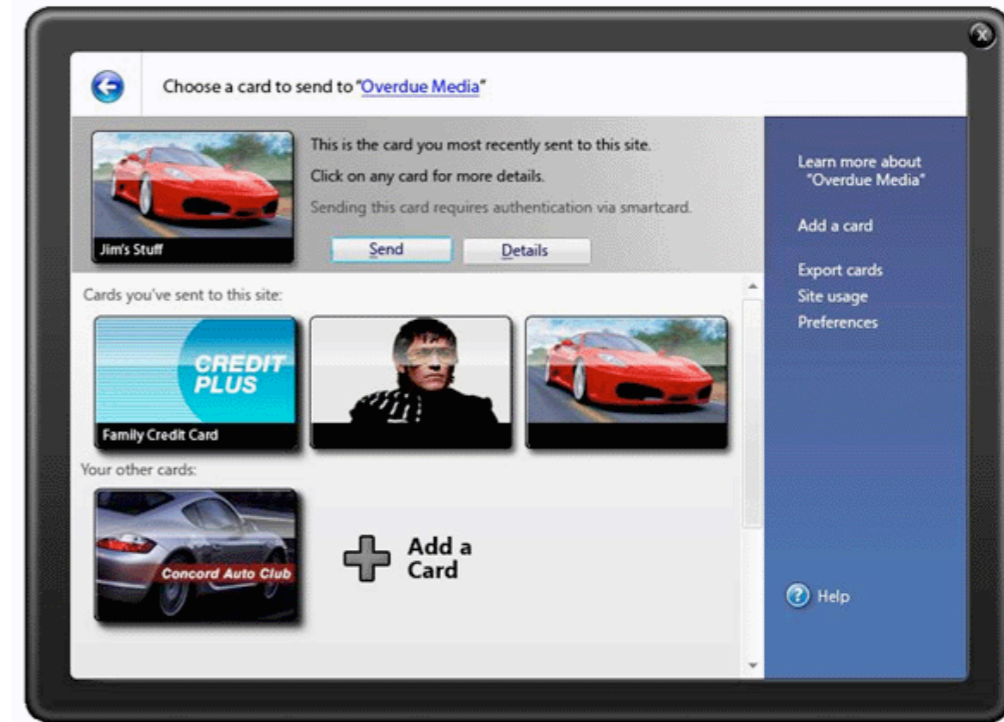
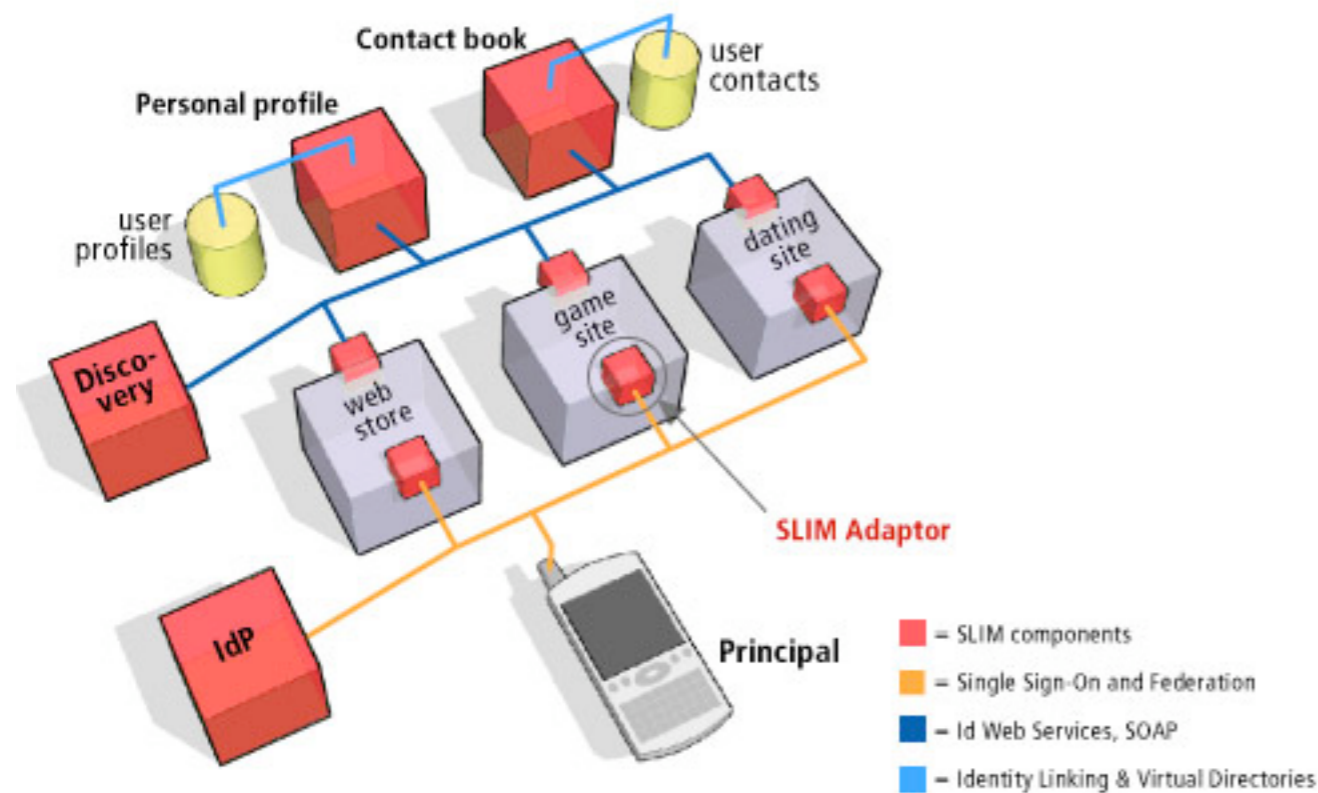
3 Fun! Enjoy a speech from Dick about Identity 2.0



# And what about \_\_\_\_\_?



## Oasis SAML 2.0



Microsoft CardSpace (WS-\*)



Microsoft Live ID (Passport)

# That's it



Got it?

Slides on: [keepthebyte.ch](http://keepthebyte.ch)

Links on: [del.icio.us/keepthebyte/openid](https://del.icio.us/keepthebyte/openid)