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?

local.ch

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)

local.ch

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

local.ch

how much can I depend on you?

trust

vs.

control

how much information am I going to give?

local.ch

SSO
Single-Sign-On

using the same credentials to access multiple services
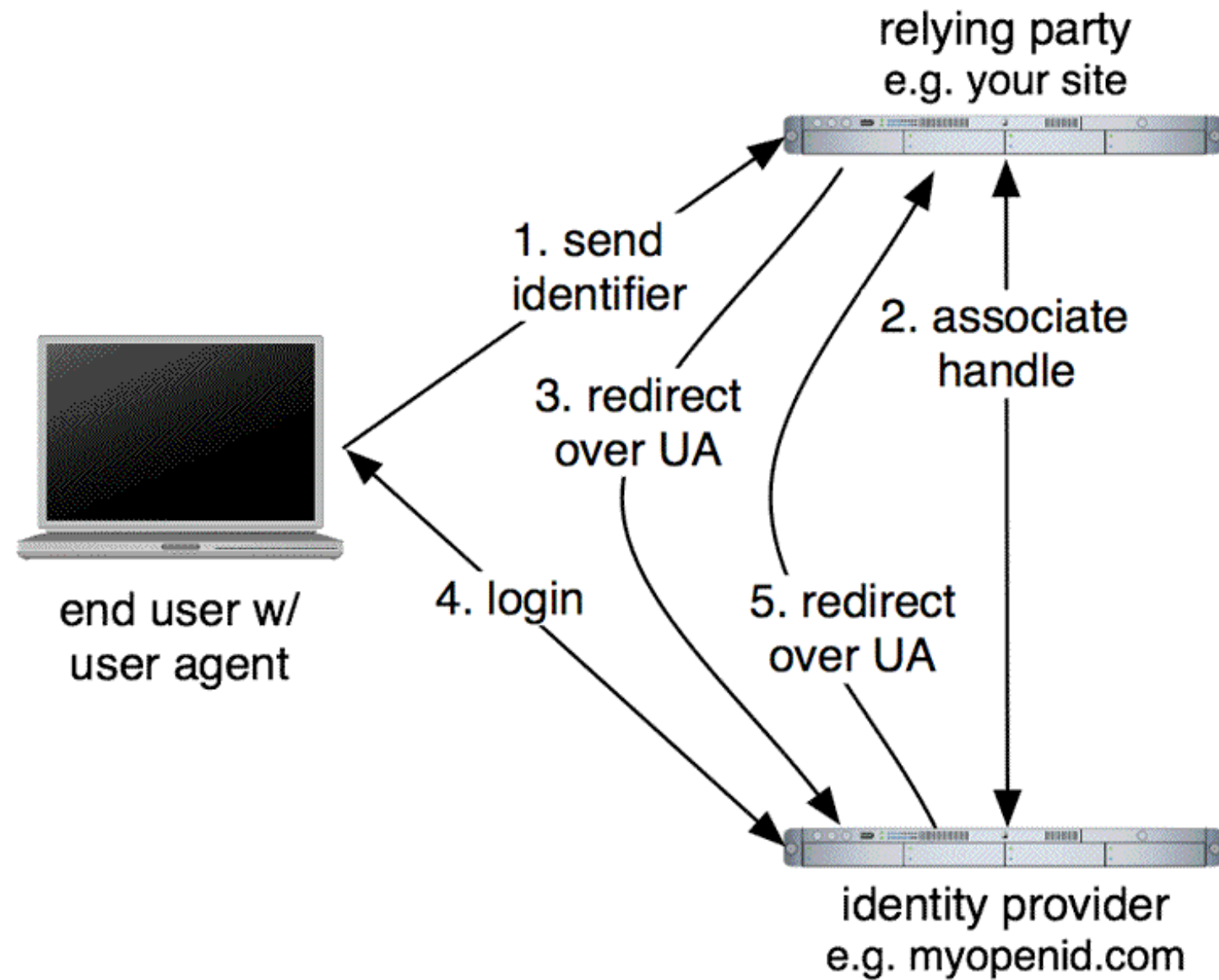
automatic authentication beyond session and service

local.ch

OpenID
and friends.

Authentication

Identity

SSO

local.ch

Use a URI* as Username!

I own keepthebyte.ch

    - why not using it as my global username?
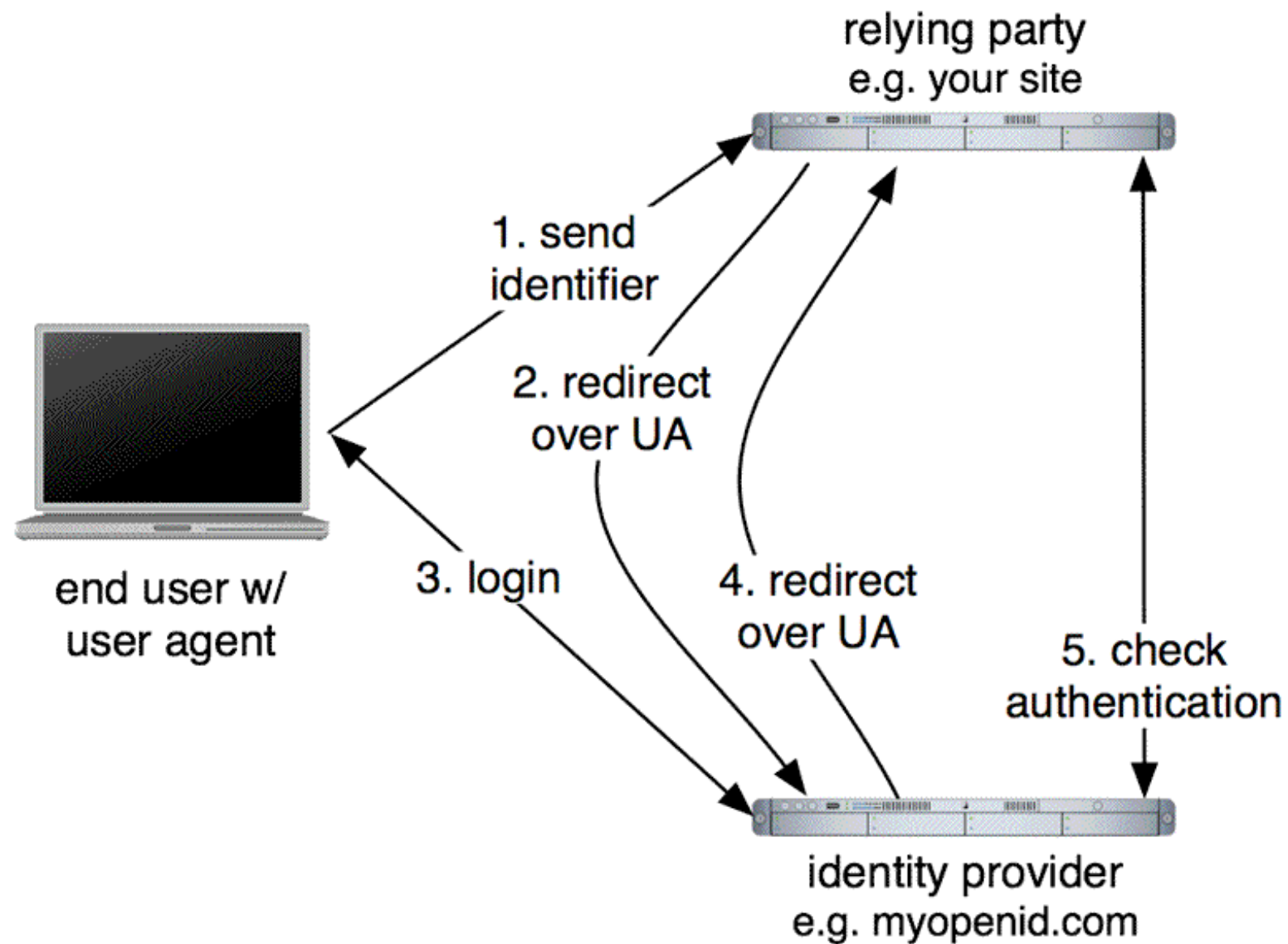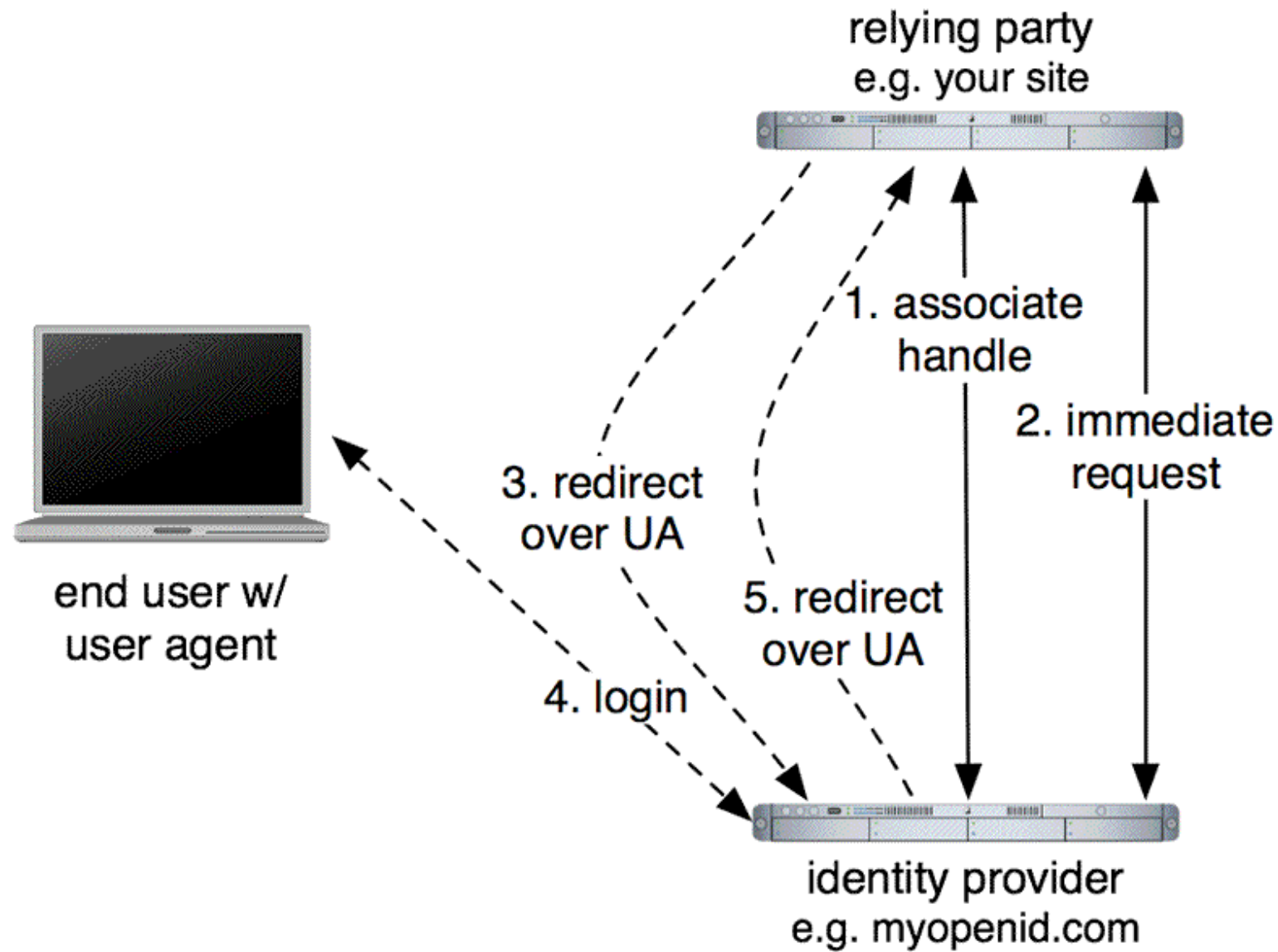
local.ch

Time for a demo...

Process Overview

relying party
e.g. your site

1. send
identifier

2. associate
handle

3. redirect
over UA

end user w/
user agent

4. login

5. redirect
over UA

identity provider
e.g. myopenid.com

...with Auto Login

relying party
e.g. your site

1. send identifier

2. associate handle

3. redirect over UA

4. redirect over UA

end user w/ user agent

identity provider
e.g. myopenid.com

local.ch

...Stateless (Dump Mode)

relying party
e.g. your site

1. send identifier

2. redirect over UA

end user w/ user agent

3. login

4. redirect over UA

5. check authentication

identity provider
e.g. myopenid.com

Not recommended due Security Issue!

... Instant (Immediate Mode)

relying party
e.g. your site

1. associate handle

2. immediate request

3. redirect over UA

5. redirect over UA

4. login

end user w/ user agent

identity provider
e.g. myopenid.com

local.ch

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

local.ch✛

Properties Exchange

Manage personal profile information centrally on the OpenID Provider site

Maybe even have multiple Persona - like MyOpenID is offering

Persona Name	Default
	☑ Make this my default persona
	☐ Make this my public persona
Nickname	keepthebyte
Full Name	Cédric Hüsler
E-mail Address	myopenid@keepthebyte.com
Birth Date	Month ⬍ Day ⬍ Year ⬍
Postal Code	
Gender	-- ⬍
Country	Switzerland ⬍
Time Zone	Europe/Zurich ⬍
Preferred Language	English ⬍

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

Default   edit

Nickname	keepthebyte
Full Name	Cédric Hüsler
E-mail Address	myopenid@keepthebyte.com
Country	CH
Time Zone	Europe/Zurich
Preferred Language	EN

(Allow Forever) (Allow Once) (Deny)

local.ch✚

Implementation

OpenID Providers

- MyOpenID.com, VeriSign PIP, ...
- List: openid.net/wiki/index.php/Public_OpenID_providers

Specification

- openid.net

List of Libraries & Enabled Software

- openid.net/wiki/index.php/Libraries
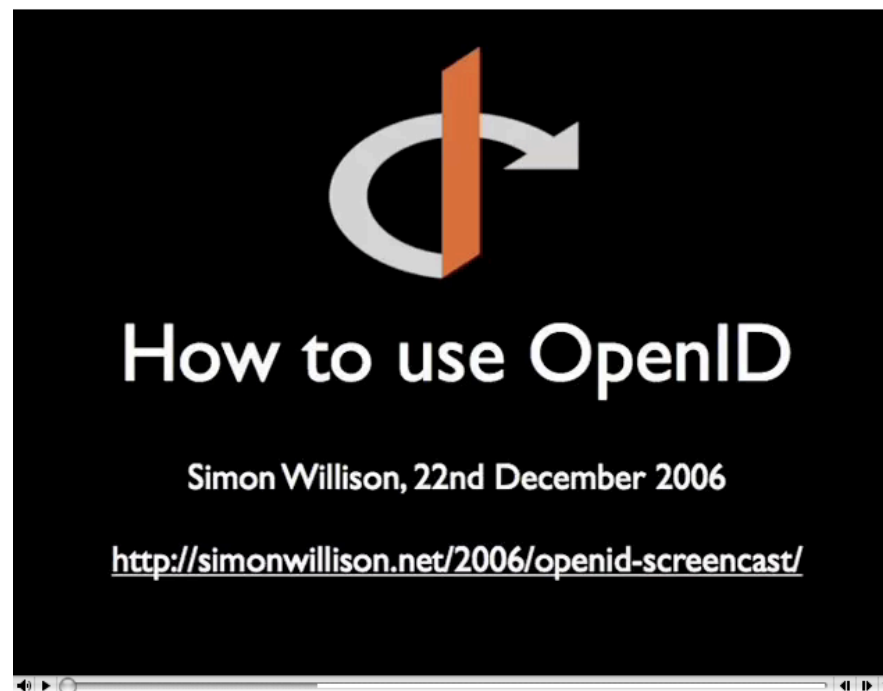
local.ch

And You?

1 Create your own OpenID

2 Make your blog/site OpenID ready!
A good starting point is to allow users to sign
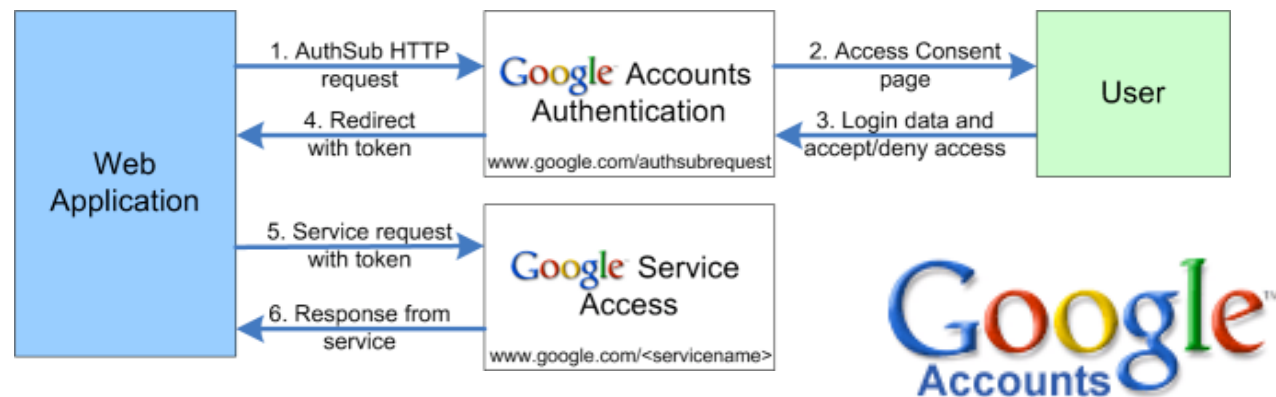comments and leave ratings with OpenID

O'REILLY
ETech
EMERGING
TECHNOLOGY
CONFERENCE
MARCH 6-9, 2006
MANCHESTER GRAND HYATT
SAN DIEGO, CALIFORNIA

Who is the Dick
on your site?

3 Fun! Enjoy a speech from Dick
about Identity 2.0

4 Show friends how it works...

How to use OpenID

Simon Willison, 22nd December 2006

http://simonwillison.net/2006/openid-screencast/

local.ch

And what about _____?

Oasis SAML 2.0
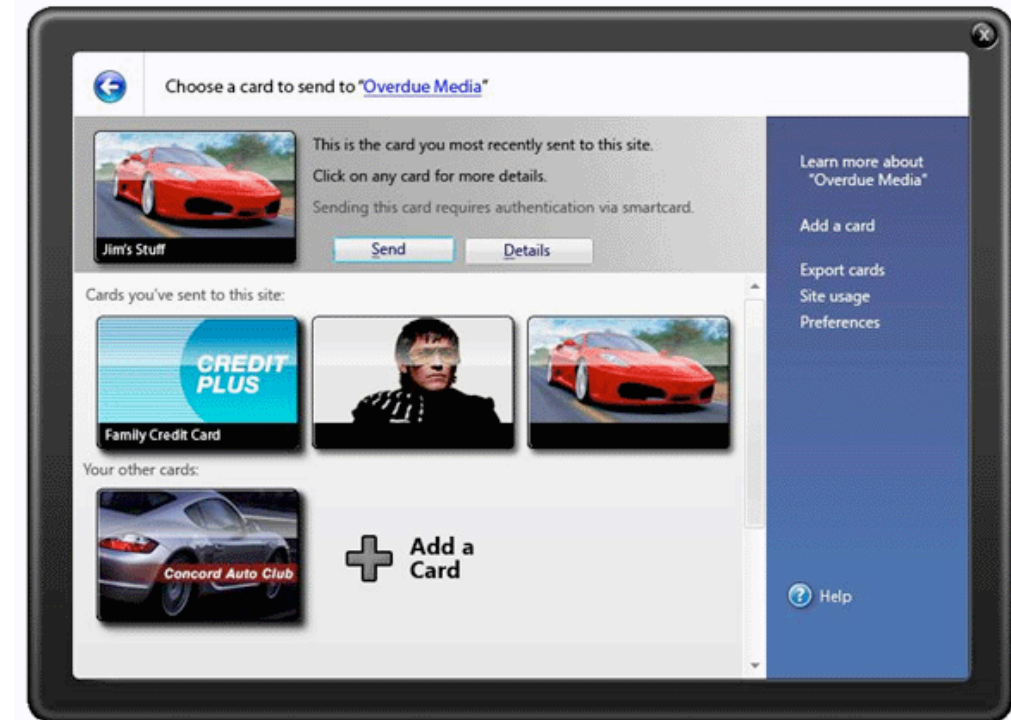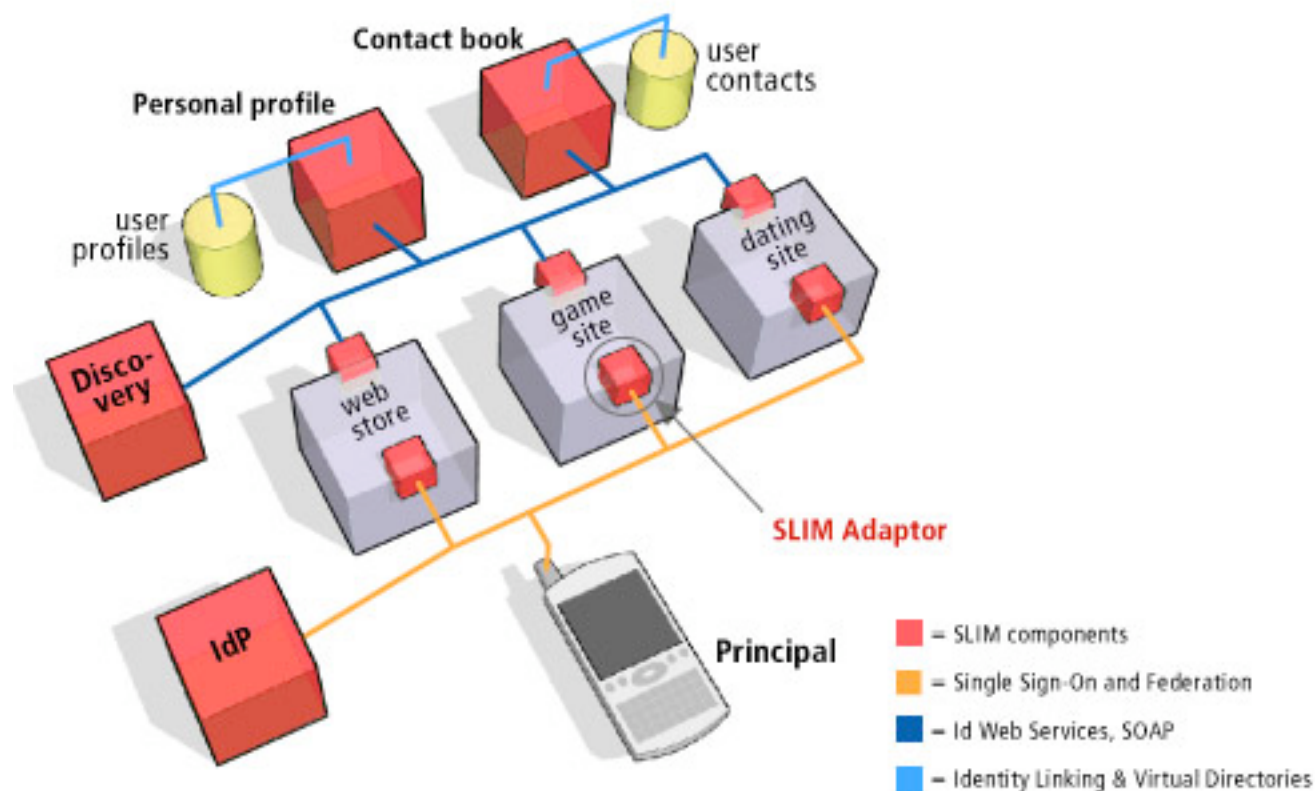
Microsoft CardSpace (WS-*)

Microsoft Live ID (Passport)

local.ch

That's it

Got it?

Slides on: keepthebyte.ch

Links on: del.icio.us/keepthebyte/openid

local.ch