Enabling Identity 2.0 in Java Technology

David Recordon and Hans Granqvist

Innovation Group
VeriSign, Inc.
http://verisignlabs.com

TS-6536

Why Spend an Hour With Us?

Web 2.0 changes identity online

Learn how to use it in Java™ platform

Agenda

What is Web 2.0 and Identity 2.0?

OpenID explained

A Java platform OpenID library

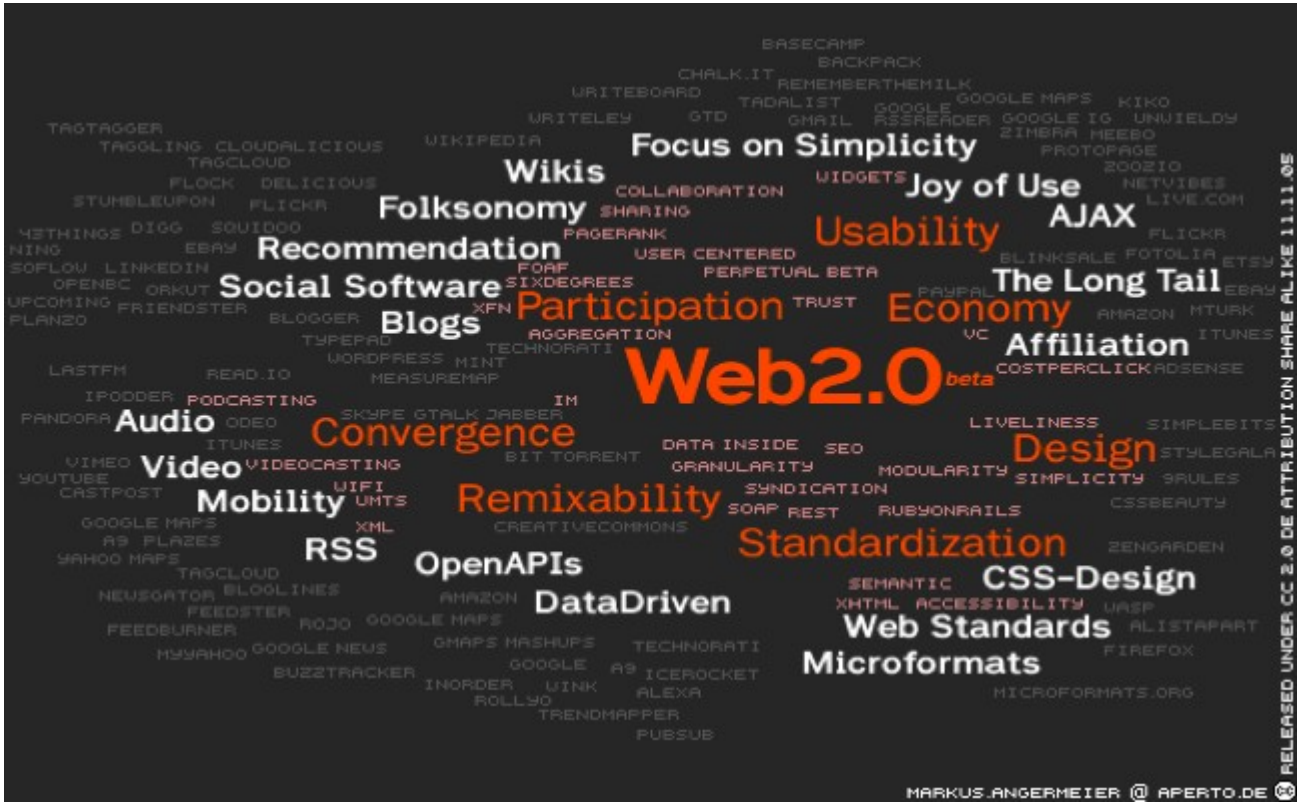
Agenda

What is Web 2.0 and Identity 2.0?

OpenID explained

A Java platform OpenID library

Web 2.0


Web2.0
beta
Focus on Simplicity
Wikis
Folksonomy
Usability
Joy of Use
AJAX
Recommendation
Social Software
Participation
Economy
The Long Tail
Blogs
Affiliation
Audio
Convergence
Design
Video
Mobility
Remixability
Standardization
RSS
OpenAPIs
DataDriven
CSS-Design
Web Standards
Microformats
MARKUS.ANGERMEIER @ APERTO.DE
RELEASED UNDER CC 2.0 DE ATTRIBUTION SHARE ALIKE 11.11.05

What Does That Mean?

- Users in control
- Data sharing
- Social collaboration
- Lightweight business models
- Perpetual beta
- Application platform

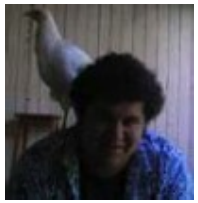
Online Identity

David Recordon

Daveman692

david@simplemachines.org

recordond@gmail.com

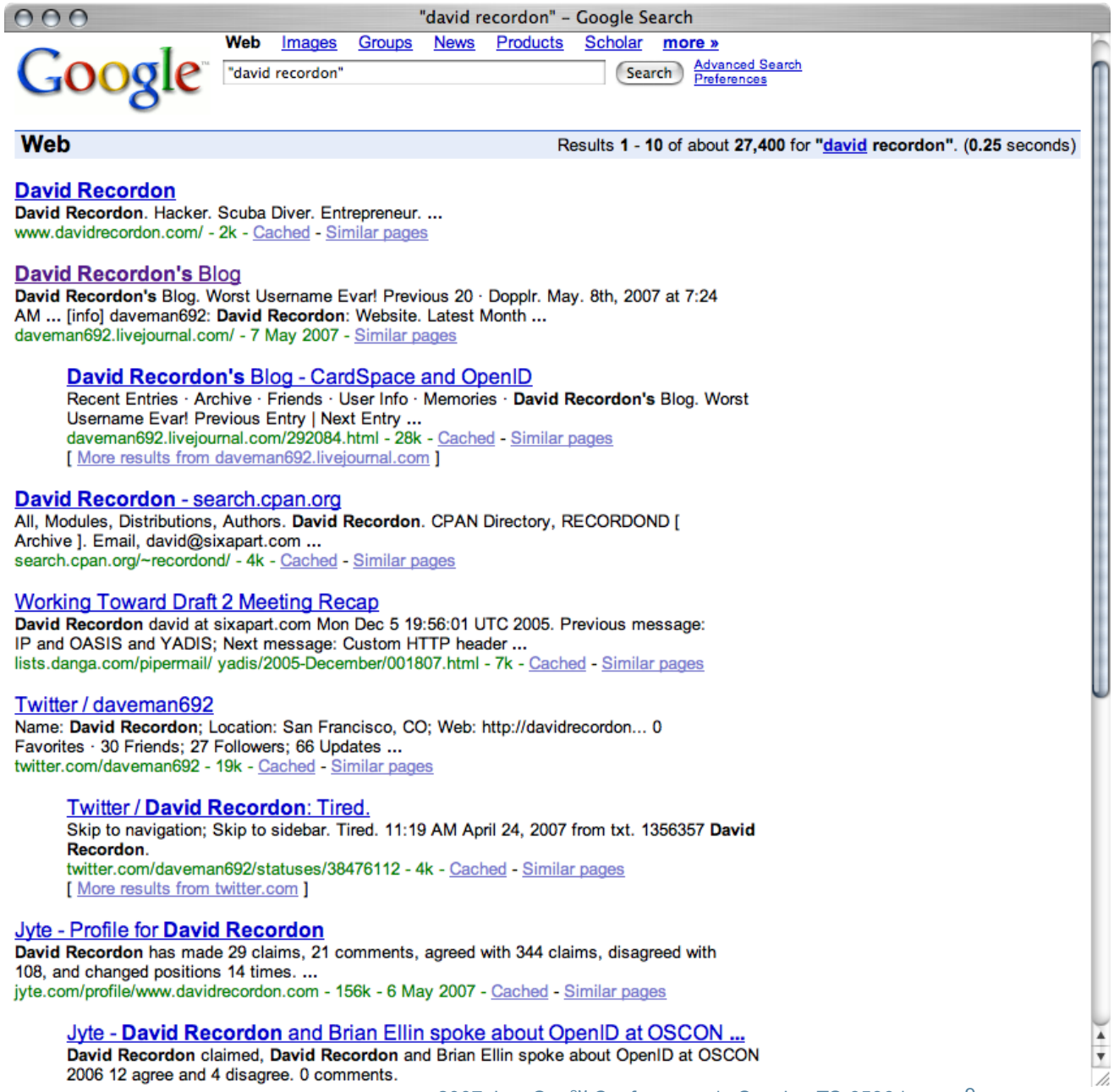


Online Identity

http://daveman692.livejournal.com

recordond

drecordon@verisign.com


"david recordon" – Google Search
Google
Web Images Groups News Products Scholar more »
"david recordon"
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 27,400 for "david recordon". (0.25 seconds)
David Recordon
David Recordon. Hacker. Scuba Diver. Entrepreneur. ...
www.davidrecordon.com/ - 2k - Cached - Similar pages
David Recordon's Blog
David Recordon's Blog. Worst Username Evar! Previous 20 · Dopplr. May. 8th, 2007 at 7:24 AM ... [info] daveman692: David Recordon: Website. Latest Month ...
daveman692.livejournal.com/ - 7 May 2007 - Similar pages
David Recordon's Blog - CardSpace and OpenID
Recent Entries · Archive · Friends · User Info · Memories · David Recordon's Blog. Worst Username Evar! Previous Entry | Next Entry ...
daveman692.livejournal.com/292084.html - 28k - Cached - Similar pages
[More results from daveman692.livejournal.com]
David Recordon - search.cpan.org
All, Modules, Distributions, Authors. David Recordon. CPAN Directory, RECORDOND [Archive]. Email, david@sixapart.com ...
search.cpan.org/~recordond/ - 4k - Cached - Similar pages
Working Toward Draft 2 Meeting Recap
David Recordon david at sixapart.com Mon Dec 5 19:56:01 UTC 2005. Previous message: IP and OASIS and YADIS; Next message: Custom HTTP header ...
lists.danga.com/pipermail/ yadis/2005-December/001807.html - 7k - Cached - Similar pages
Twitter / daveman692
Name: David Recordon; Location: San Francisco, CO; Web: http://davidrecordon... 0 Favorites · 30 Friends; 27 Followers; 66 Updates ...
twitter.com/daveman692 - 19k - Cached - Similar pages
Twitter / David Recordon: Tired.
Skip to navigation; Skip to sidebar. Tired. 11:19 AM April 24, 2007 from txt. 1356357 David Recordon.
twitter.com/daveman692/statuses/38476112 - 4k - Cached - Similar pages
[More results from twitter.com]
Jyte - Profile for David Recordon
David Recordon has made 29 claims, 21 comments, agreed with 344 claims, disagreed with 108, and changed positions 14 times. ...
jyte.com/profile/www.davidrecordon.com - 156k - 6 May 2007 - Cached - Similar pages
Jyte - David Recordon and Brian Ellin spoke about OpenID at OSCON ...
David Recordon claimed, David Recordon and Brian Ellin spoke about OpenID at OSCON 2006 12 agree and 4 disagree. 0 comments.

claimID : Fred Stutzman

register | login

Viewing 27 links

Personal

The best place to start to find out about me.

My Blog - Unit Structures - *Verified*

About Me | By Me | Tagged with: blog writing academic

Thoughts about information, social networks, identity and technology.

My Homepage - Fred Stutzman at ibiblio.org - *Verified*

About Me | By Me | Tagged with: ibiblio academic personal

I worked for ibiblio prior to claimID, and I maintain my homepage there.

My del.icio.us Links - del.icio.us/fstutzman

About Me | By Me | Tagged with: links

My Flickr Photos

About Me | By Me | Tagged with: photos media pictures

Projects

I work (or have worked) on these projects.

claimID.com - Manage your online identity

About Me | By Me | Tagged with: claimid projects

Terrell Russell and I started claimID.com, with graphic design by Kelly Marks. We were supported by our friends, family, and colleagues at SILS-UNC. ClaimID is the coolest thing ever.

Lyceum.ibiblio.org

About Me | Managed by me | Tagged with: ibiblio lyceum

Lyceum is an enterprise-class multi-user, multi-blog branch of Wordpress. I'm responsible for the

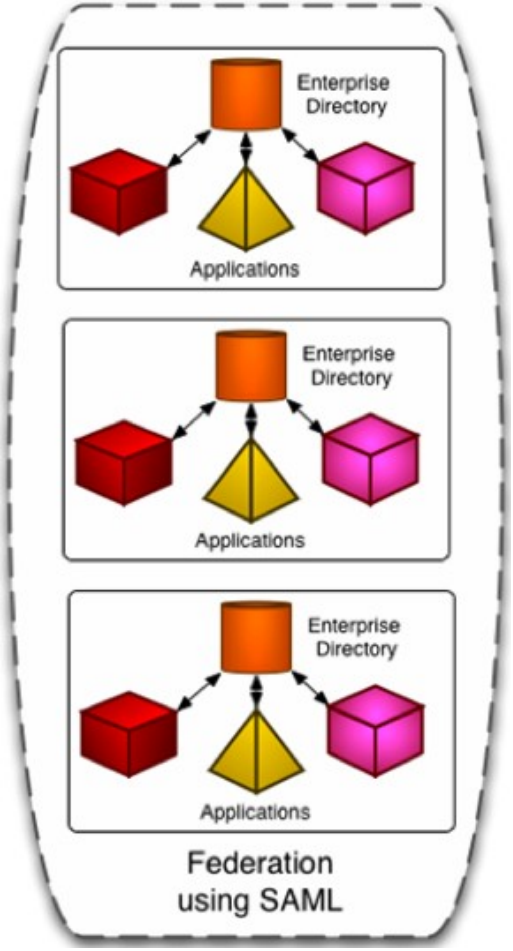
Fred Stutzman
ClaimID.com
200 Oak Ave.
Carrboro, NC 27510
(919) 260-8508

I am a Ph.D. student at the University of North Carolina, and the co-founder of ClaimID. Originially from Albany, NY, I am currently located in Chapel Hill, North Carolina.

My academic interests include identity representation, social software, the net-generation, and social effects of technology. One day I'll figure out how that all ties together. ClaimID, created with Terrell Russell, is a step in that direction.

Identity 1.0

- Walled Gardens
- AOL
- Microsoft
- Yahoo!
- Google
- Little user choice
- Many usernames
- Few passwords



User-centric Identity ("Identity 2.0")

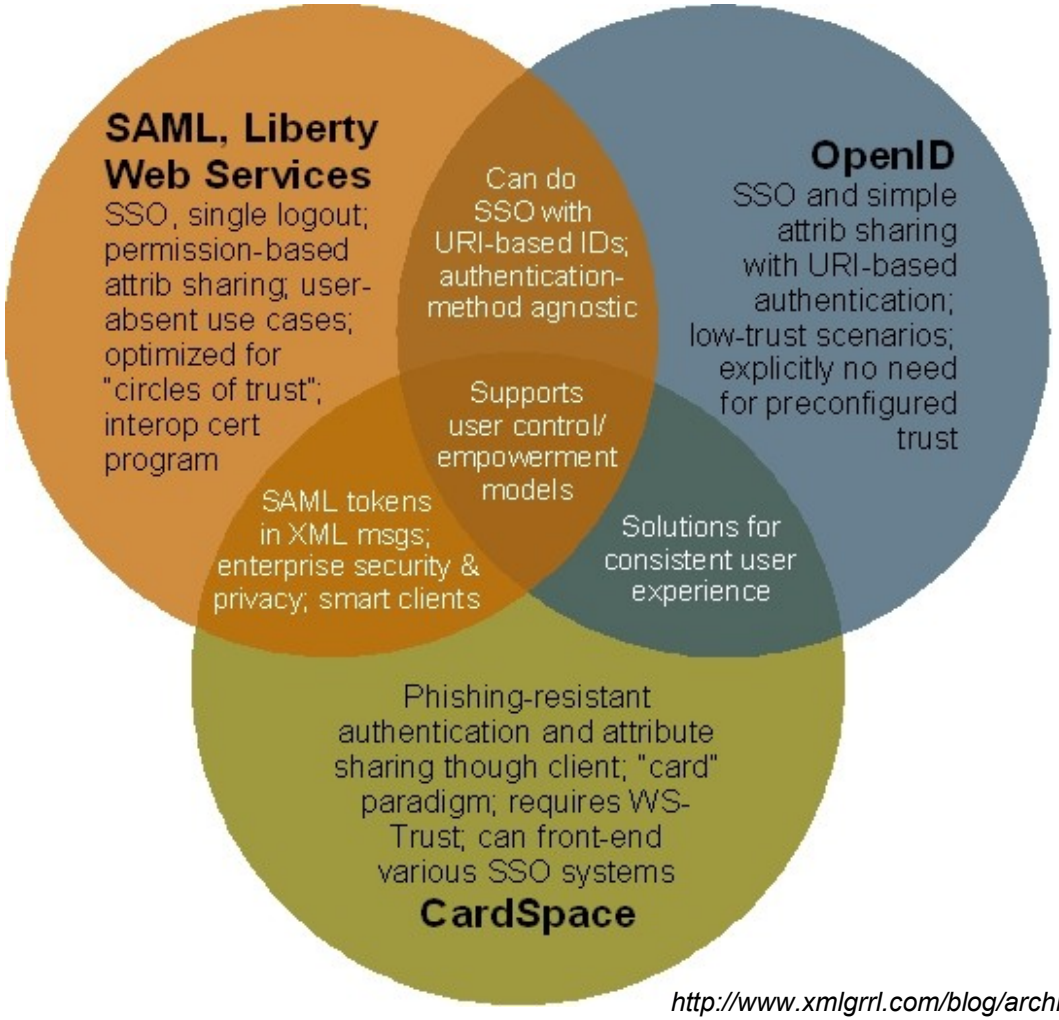
- Internet scale
- Privacy protecting
- Easy to adopt
- Community-driven

Supporting the Web as an Application Platform

So What?

- Gives user generated content meaning
- Allows for distributed reputation
  - Personal brand
- One (or more) pseudonyms
  - It isn't always about knowing "who"
- Bridging contexts

Core Technologies



http://www.xmlgrrl.com/blog/archives/2007/03/28/the-venn-of-identity/

In Summary

- Identity online is changing
- Keeping track of your digital self is difficult
- Identity 2.0 is about putting the user in control
- Various technological approaches stemming from different initial problems
- Choose the one that best fits your requirements
- Remember that these protocols can be complimentary to each other

Agenda

What is Web 2.0 and Identity 2.0?

OpenID explained

A Java platform OpenID library

“Making the Web Suck Less!”

A Few Key Bits

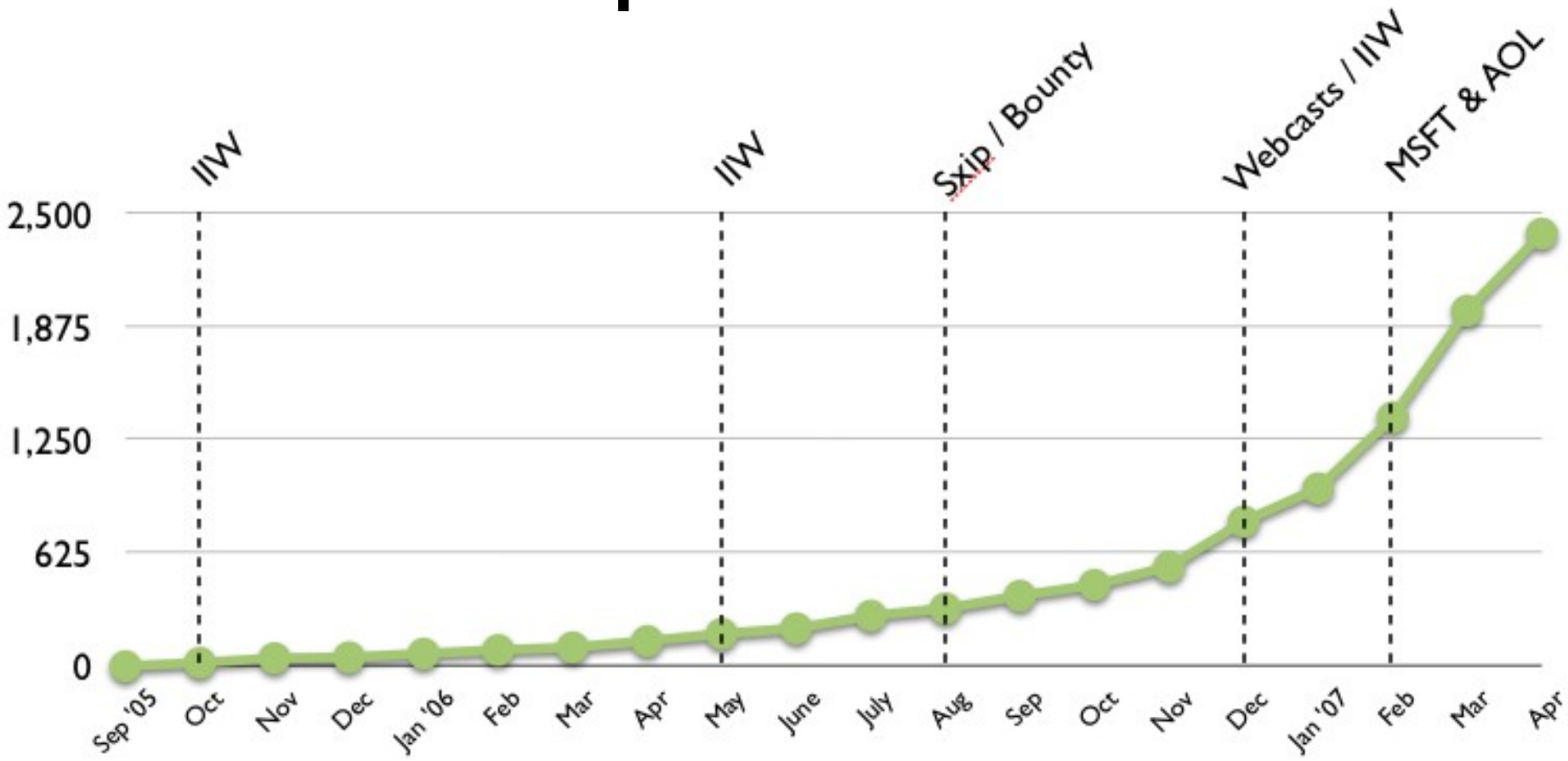
- OpenID is fully decentralized
- OpenID proves you control a URI
  - e.g., http://www.davidrecordon.com
- OpenID doesn't dictate authentication
  - Username/password
  - Jabber
  - Client certificates
  - DynDNS bound to your IP
  - etc.

Do People Have OpenIDs?

~ 90 Million of Them

(Including Every AOL User)

Trends in Adoption



Total Relying Parties
(a.k.a. places you can use this stuff)

OpenID 1.1 as seen by MyOpenID.com

How Does It Work?

- Three actors
  - End user
  - Relying party
  - OpenID provider
- Basic flow
  1. User enters their URI at the Relying Party
  2. RP establishes a relationship with the OP
  3. RP redirects user to OP
  4. User interacts with OP
  5. OP redirects user back to RP with signature
  6. RP verifies the signature on the assertion

Phishing

- A large problem on the Internet
- Implementing OpenID in certain manners can be phishing prone
- Use phishing resistant authentication methods
  - Client-side certificates (within the browser or CardSpace)
  - Site seal technology
  - Vidoop.com (different approach to passwords)
  - Browser integration (VeriSign's OpenID SeatBelt)
  - etc.

DEMO

OpenID in action

Why Should You Care?

- Lightweight account creation
  - Relieve “start-up fatigue”
- Pre-approved accounts
  - No more mailing digest passwords around
- Corporate SSO
  - Only allow *username.internal.vrsn.com*
- Complementary to Microformats
- Site-specific hacks
- Social whitelists

Who Else Is Caring?

And Don’t Forget…

Agenda

What is Web 2.0 and Identity 2.0?

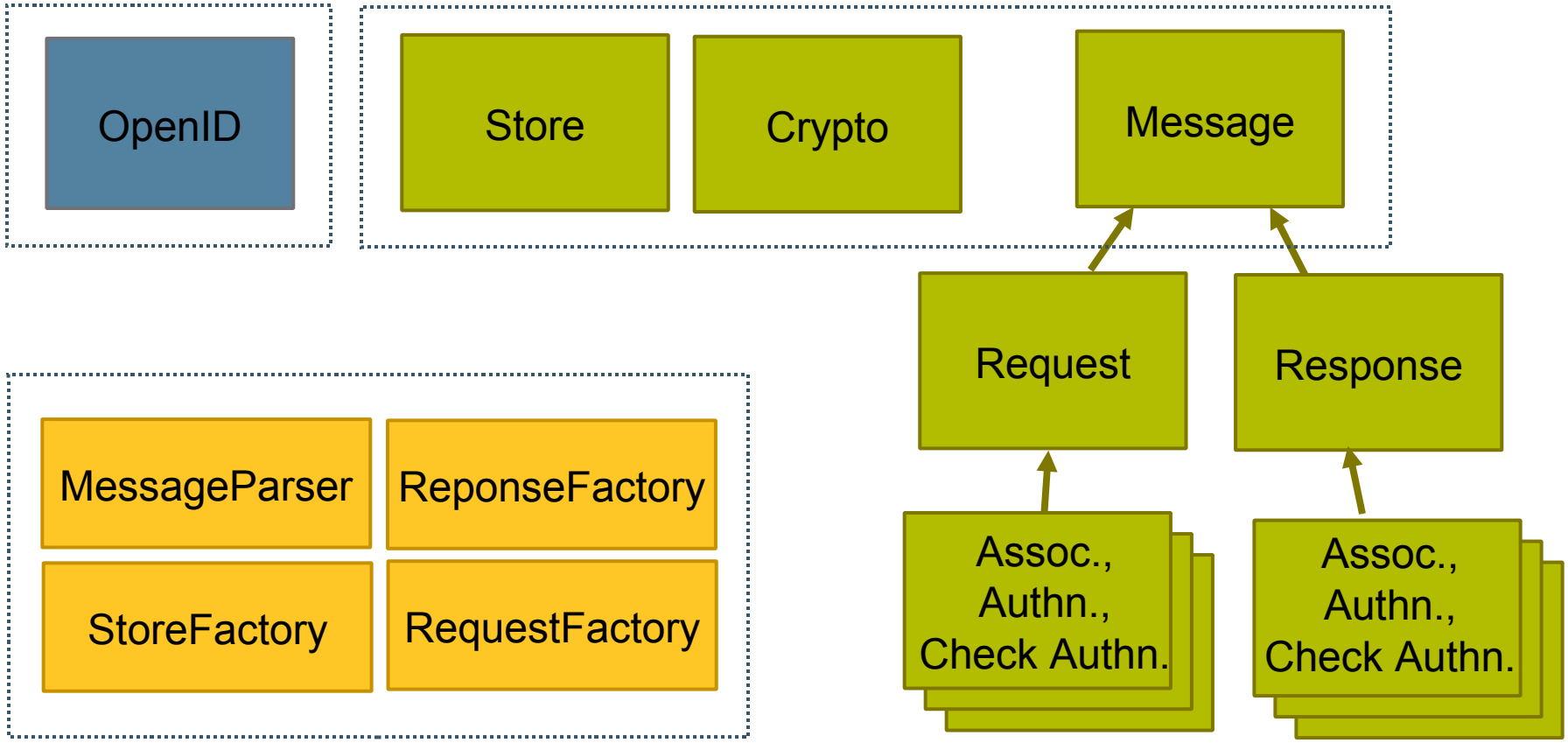
OpenID explained

A Java platform OpenID library

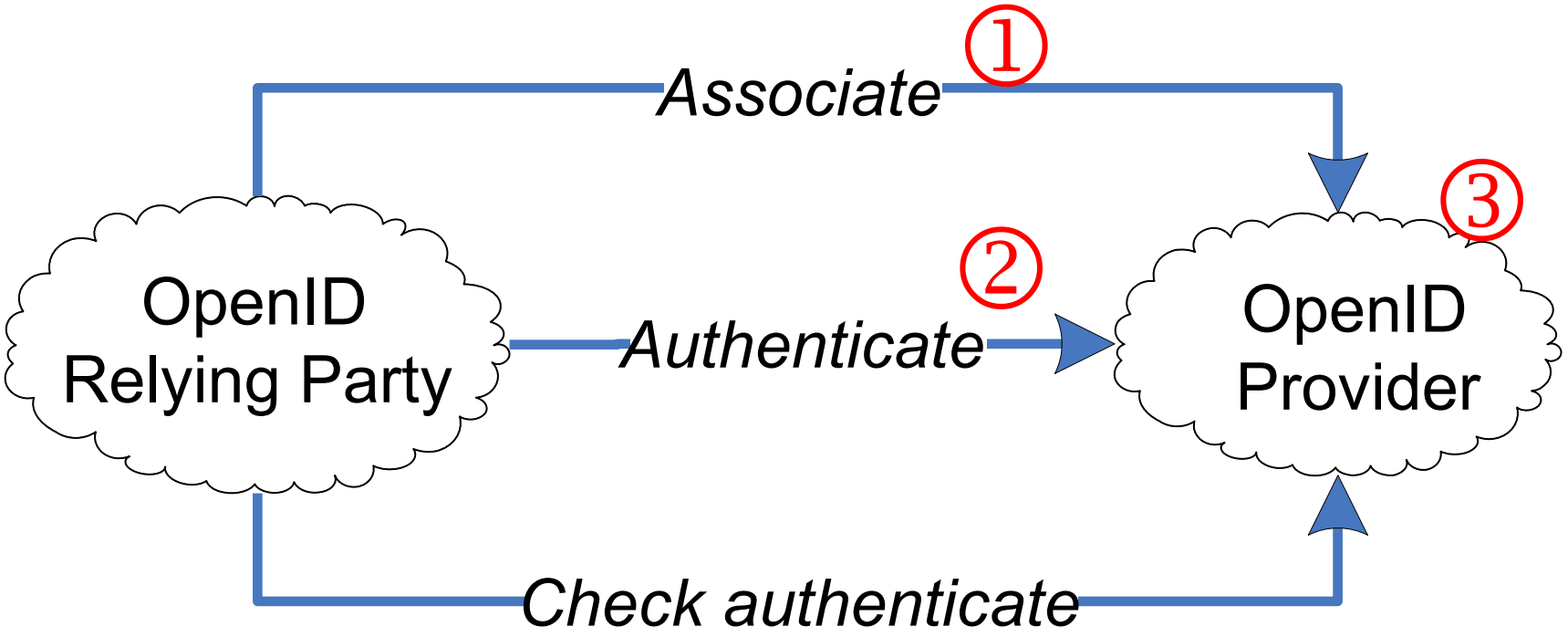
joid, a Java Platform OpenID library

- Simple & Difficult
- Providers and relying parties (consumers)
- Open source
  - http://code.google.com/p/joid
- Used in production

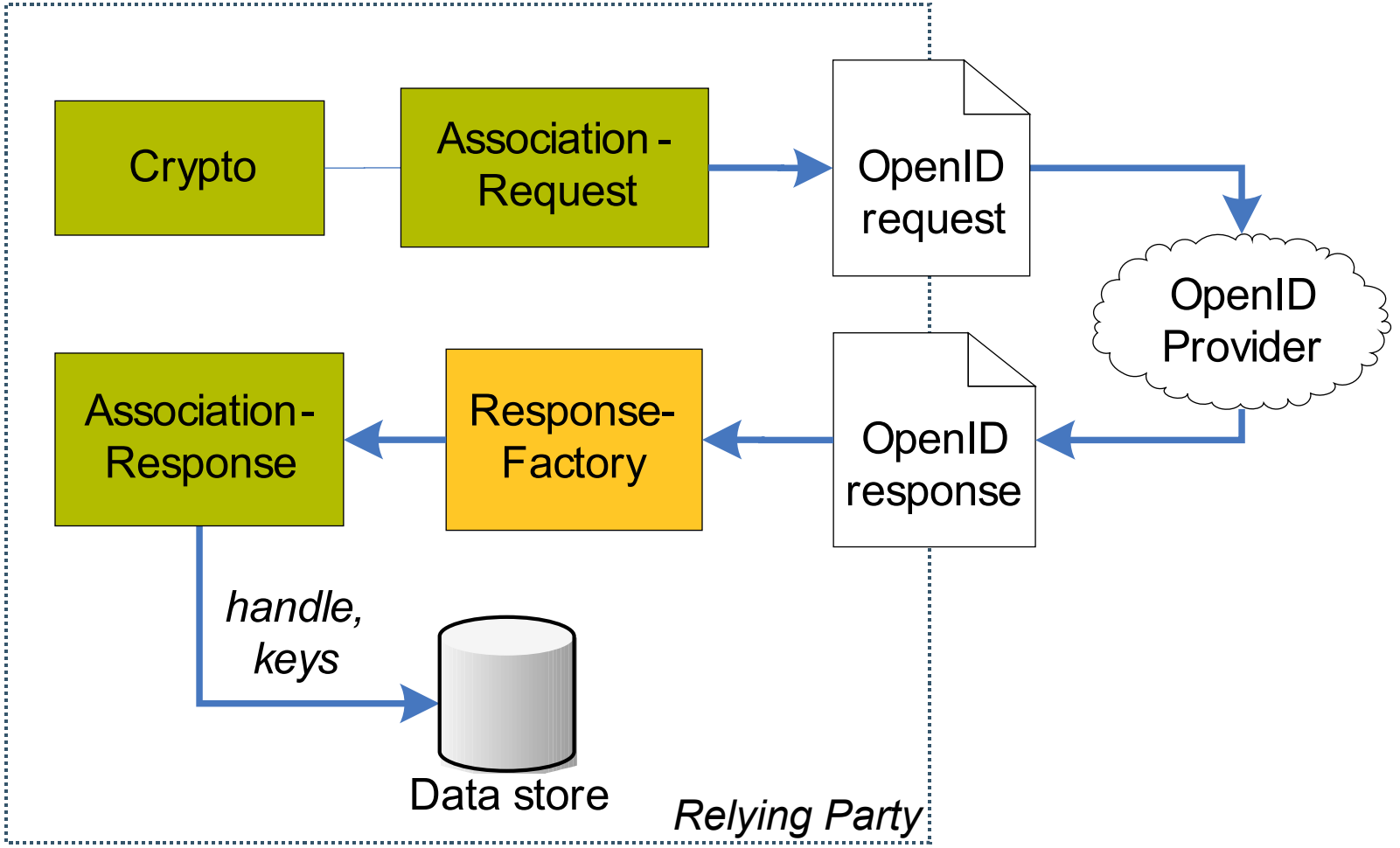
joid Building Blocks



joid Usage


①
Associate
③
②
OpenID
Relying Party
Authenticate
OpenID
Provider
Check authenticate

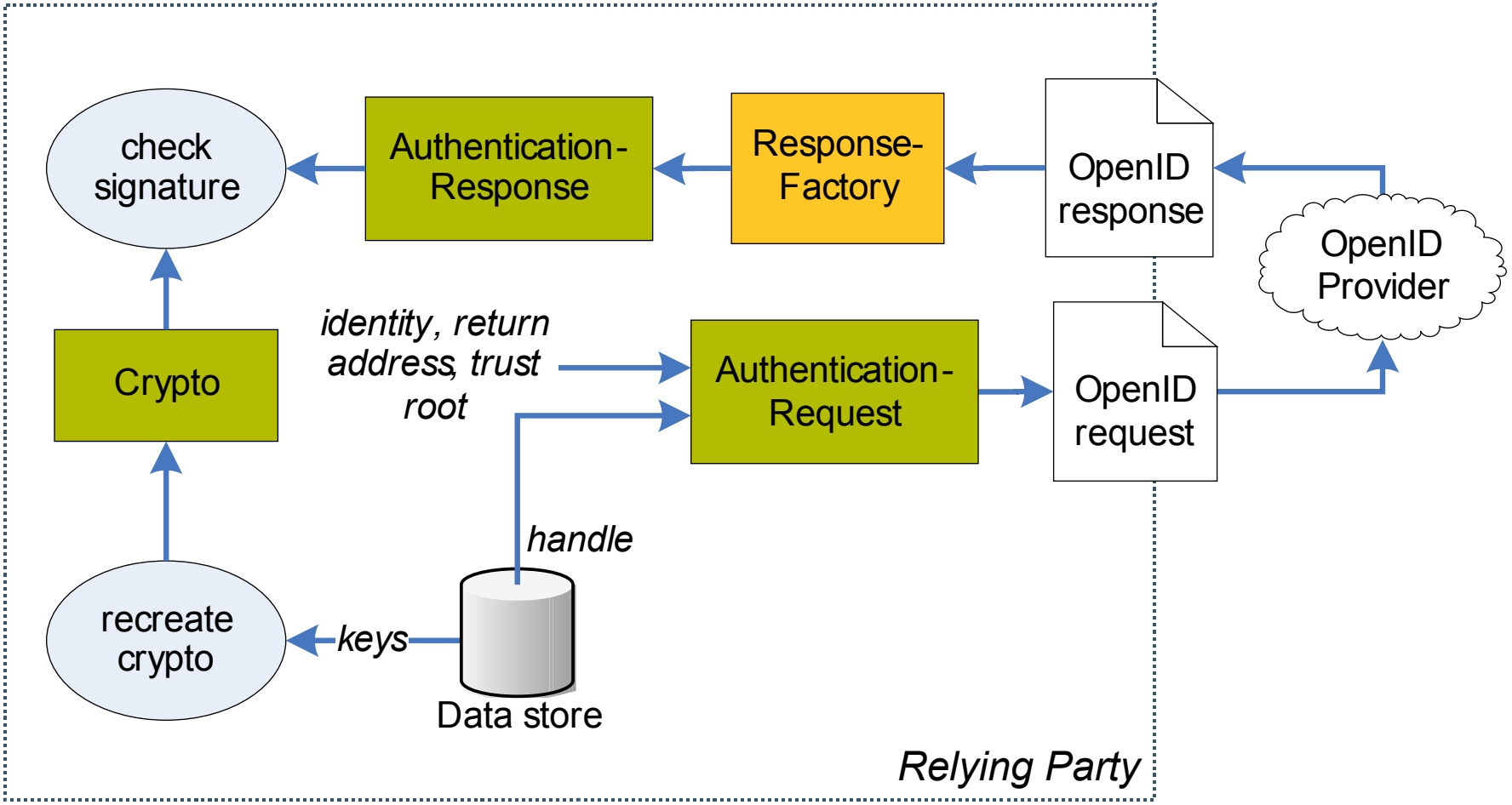
Relying Party—*Associate*



Relying Party—*Associate*

```
1. // set up crypto
2. DiffieHellman dh = DiffieHellman.getDefault();
3. Crypto crypto = new Crypto();
4. crypto.setDiffieHellman(dh);
5. // create request
6. AssociationRequest ar =
7.   AssociationRequest.create(crypto);
8. String query = ar.toUrlString();
9. // ... send request to provider, response in s
10. AssociationResponse asr =
11.  (AssociationResponse) ResponseFactory.parse(s);
12. // ... store handle, keys
```

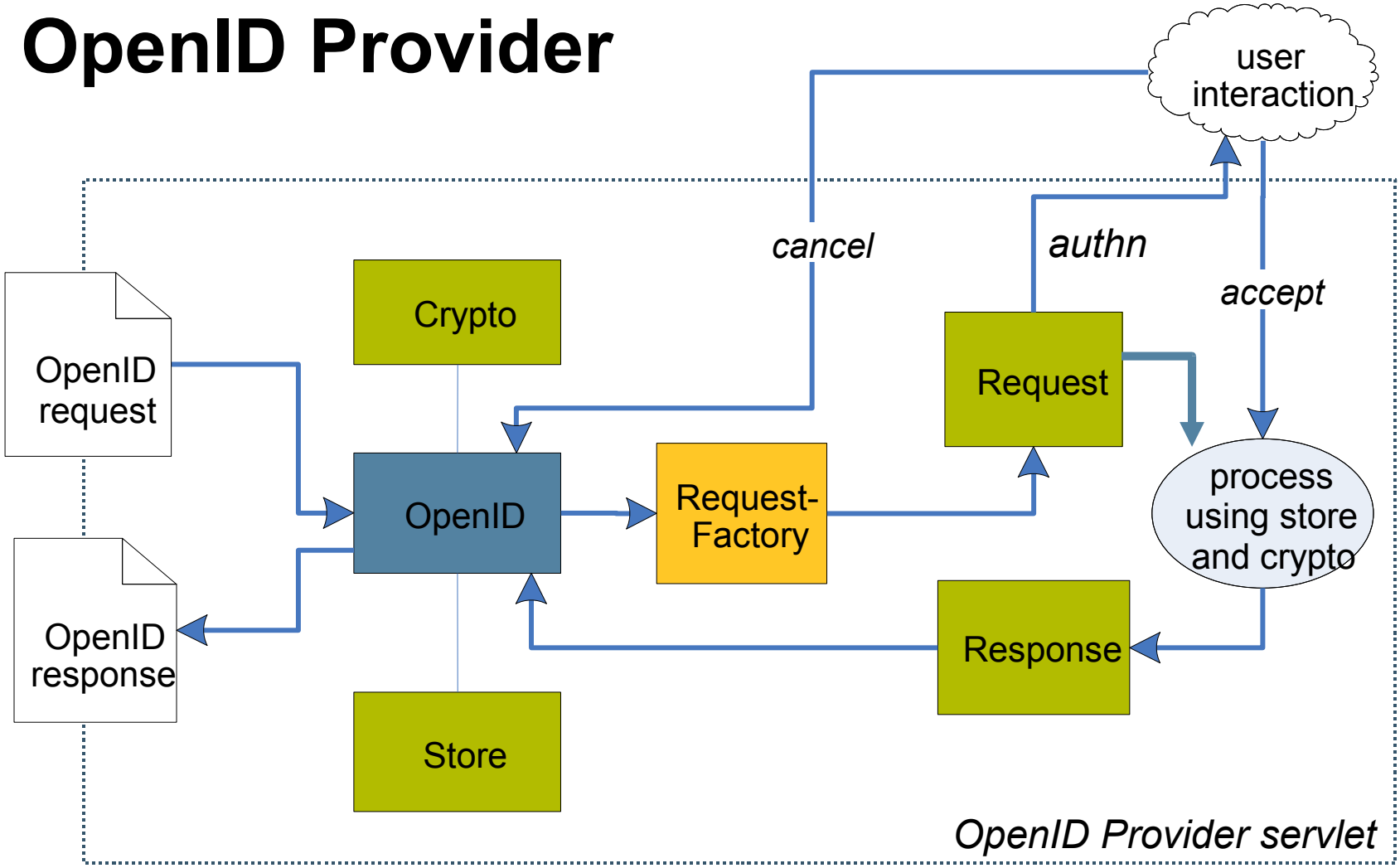
Relying Party—*Authenticate*



Relying Party—*Authenticate*

```
1. // Just like associate: Create request, send
2. // to OpenID service & parse response into 'ar'
3. // Decrypt association key
4. Crypto crypto = new Crypto();
5. DiffieHellman dh = DiffieHellman
6.       .recreate(privKey, modulus);
7. crypto.setDiffieHellman(dh);
8. byte[] key = crypto
9.       .decryptSecret(serverPublic, encryptedKey);
10. // Check signature
11. String sig = ar.getSignature();
12. String list = ar.getSignedList();
13. String check = ar.sign(key, sig);
14. // assert sig == check
```

OpenID Provider



OpenID Provider

```
1. OpenID op = new OpenId(store);
2. if (op.canHandle(query)){
3.   // if auth, ask user here & break if cancel
4.   String s = op.handleRequest(query);
5.   // if error response, set http headers
6.   if (op.isAnErrorResponse(s)){
7.     ... error, SC_BAD_REQUEST
8.   }
9.   // responses are returned differently
10.  if (op.isAuthenticationRequest(query)) {
11.    response.sendRedirect(s);
12.  } else {
13.    out.print(s);
14.  }
15. }
```

DEMO

JOID in action

Summary

- Internet identity is changing
  - Users are put in control of their data
- OpenID gains much traction
  - The Identity 2.0 system of choice
- Java platform open source library available now
  - Production-ready
  - http://code.google.com/p/joid

For More Information

- OpenID specifications
  - http://openid.net, general@openid.net
- Joid source code
  - http://code.google.com/p/joid
- Talk to us
  - David Recordon: drecordon@verisign.com
  - Hans Granqvist: hgranqvist@verisign.com

Q&A

OpenID specifications
http://openid.net

Joid source code
http://code.google.com/p/joid

David Recordon
drecordon@verisign.com,

Hans Granqvist
hgranqvist@verisign.com

Enabling Identity 2.0 in Java Technology

David Recordon and Hans Granqvist

Innovation Group
VeriSign, Inc.
http://verisignlabs.com

TS-6536