The Future of Cloud Identity Security

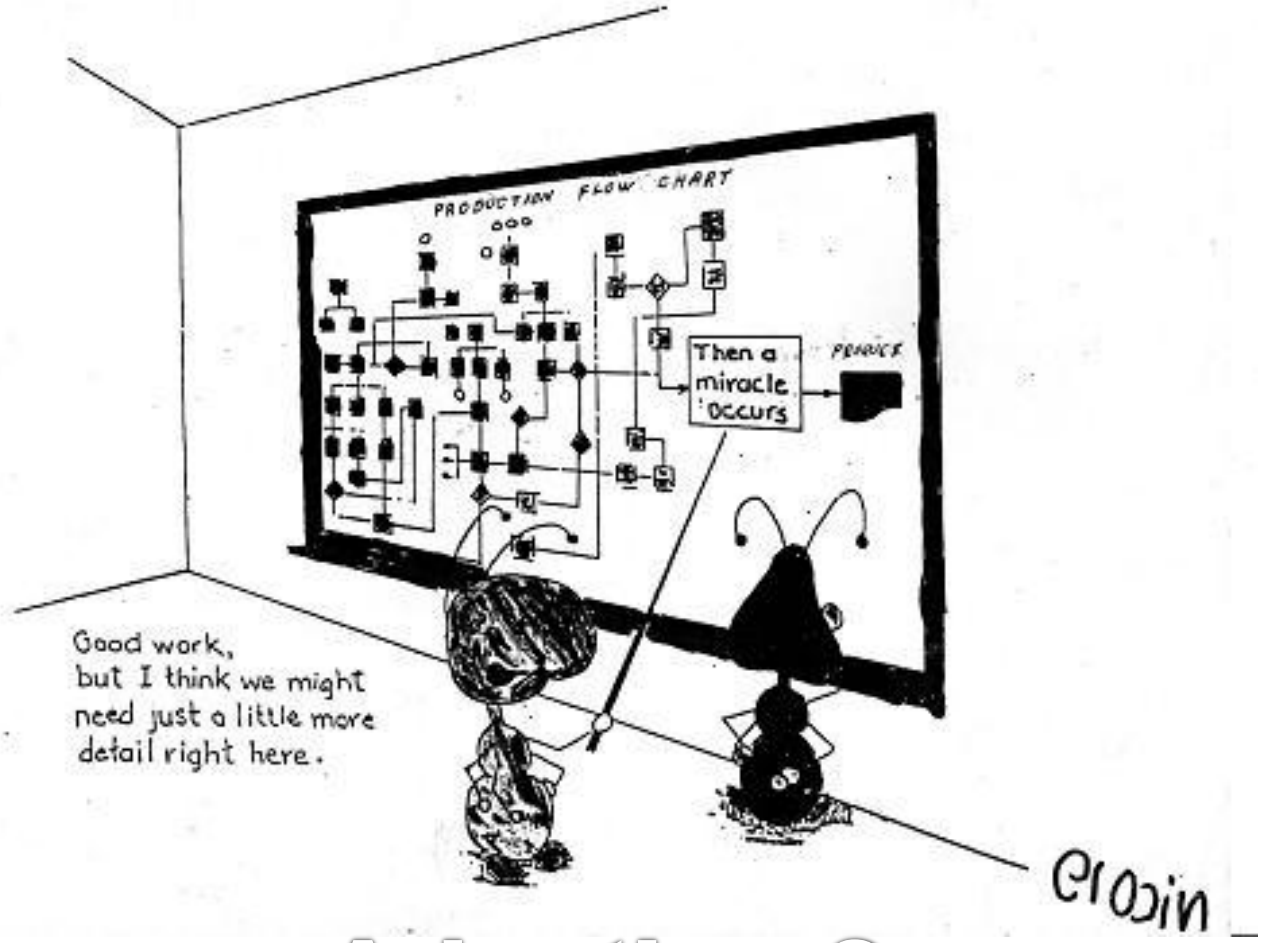
Michael Schwartz
Founder / CEO Gluu

Session ID: IAM-207
Session Classification: General Interest

RSA CONFERENCE EUROPE 2012

Background

Finally an Internet Identity Foundation…



Adoption ?

Who is behind the OpenID Foundation

Sustaining Corporate Members

Google Microsoft PayPal PingIdentity

symantec. verizon YAHOO!

Corporate Members

All Legal Documents BREATHE REPEAT BIOID be recognized ca technologies dtech Deutsche Telekom

ID BADGES facebook. gigya gluu I/DW ID/FOUNDRY

intel janrain NRI NorthID OneID otp industrial solutions

PacificEast Peercraft UnboundID WebLookOn

Non-profit Members

MITRE SWHPN FONDATION SYMPTO THERM

gluu

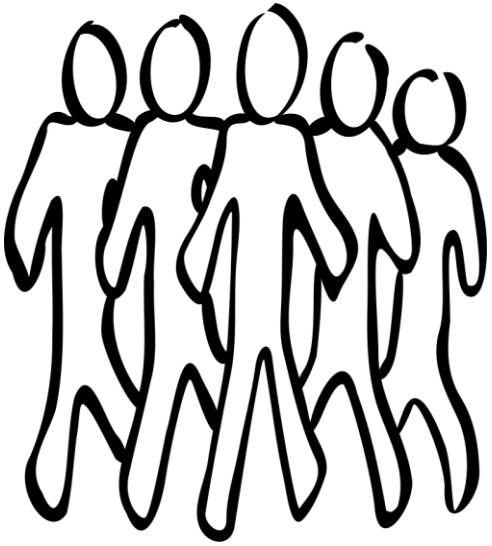
Challenges Solved by OpenID Connect

- How to share authentication with apps / websites
- Potential for Authorization
- Discovery
  - How to identify an anonymous Internet visitor
- Support constant new stream of mobile apps
  - “Apps” are not well known ahead of time… need to support dynamic registration
- Session Management
  - How can you “logout”…

How did we get here?

- 1998: Web Access Management
  - Traditional enterprise SSO (i.e. SiteMinder)
- 2001: Federation
  - How do I access websites outside my organization : SAML
- 2011 Social Login
  - Facebook Connect - Technology goes consumer

Predecessors of OpenID Connect



- SAML
  - Widely deployed by organizations
  - Authentication + attributes + federation
- OpenID
  - Easy centralized authentication
- Information Cards
  - Lots of lessons learned : OpenID Account Chooser
- OAUTH 1.0 and 1.1
  - Bundled Authentication / Authorization: first authorization

gluu

Introducing OpenID Connect

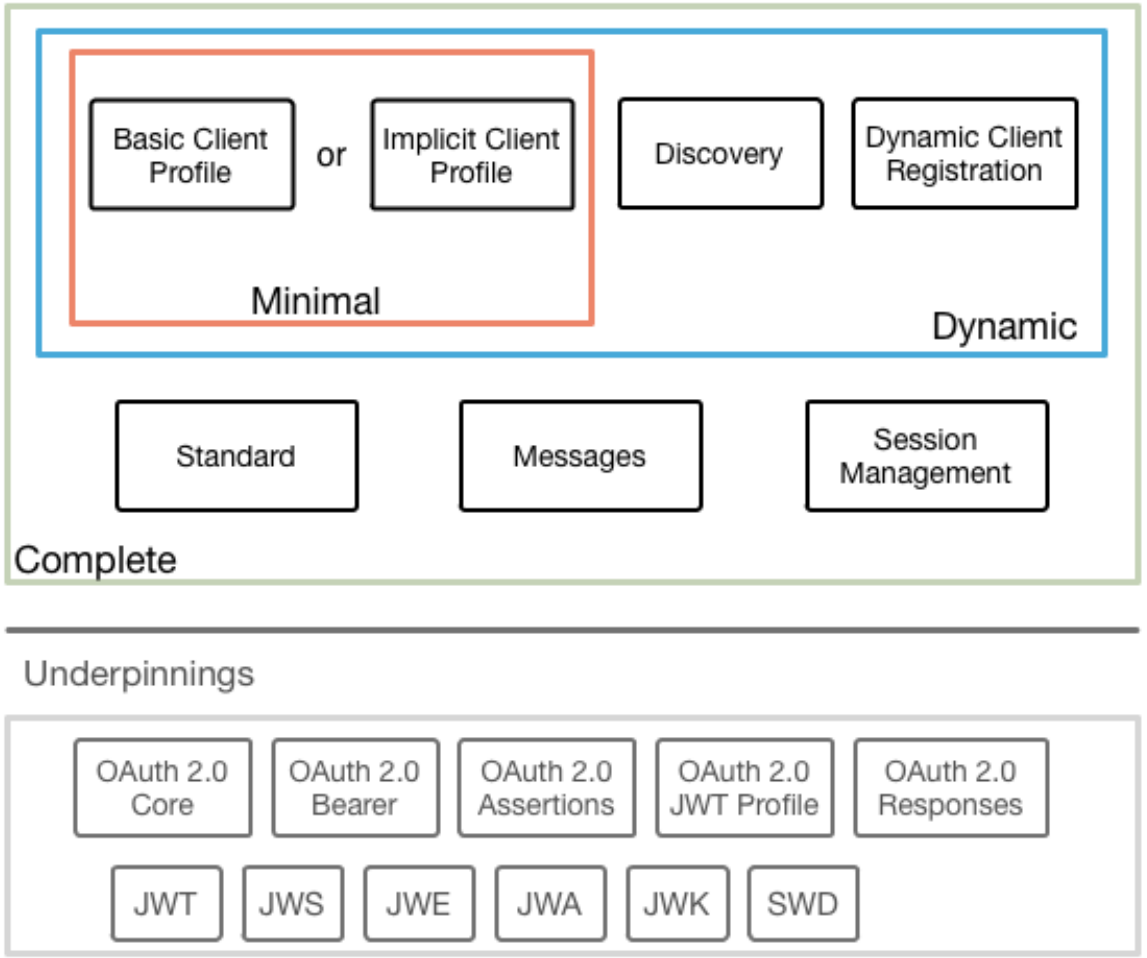
What is OpenID Connect?

- Profile of OAuth2
  - Entities
    - Client, OpenID Providers (“OP”), Relying Party (“RP”)
  - Workflows
    - Discovery, Authentication, Dynamic Client registration, Attribute Release, Session management
  - Schema
    - Token, Keystore

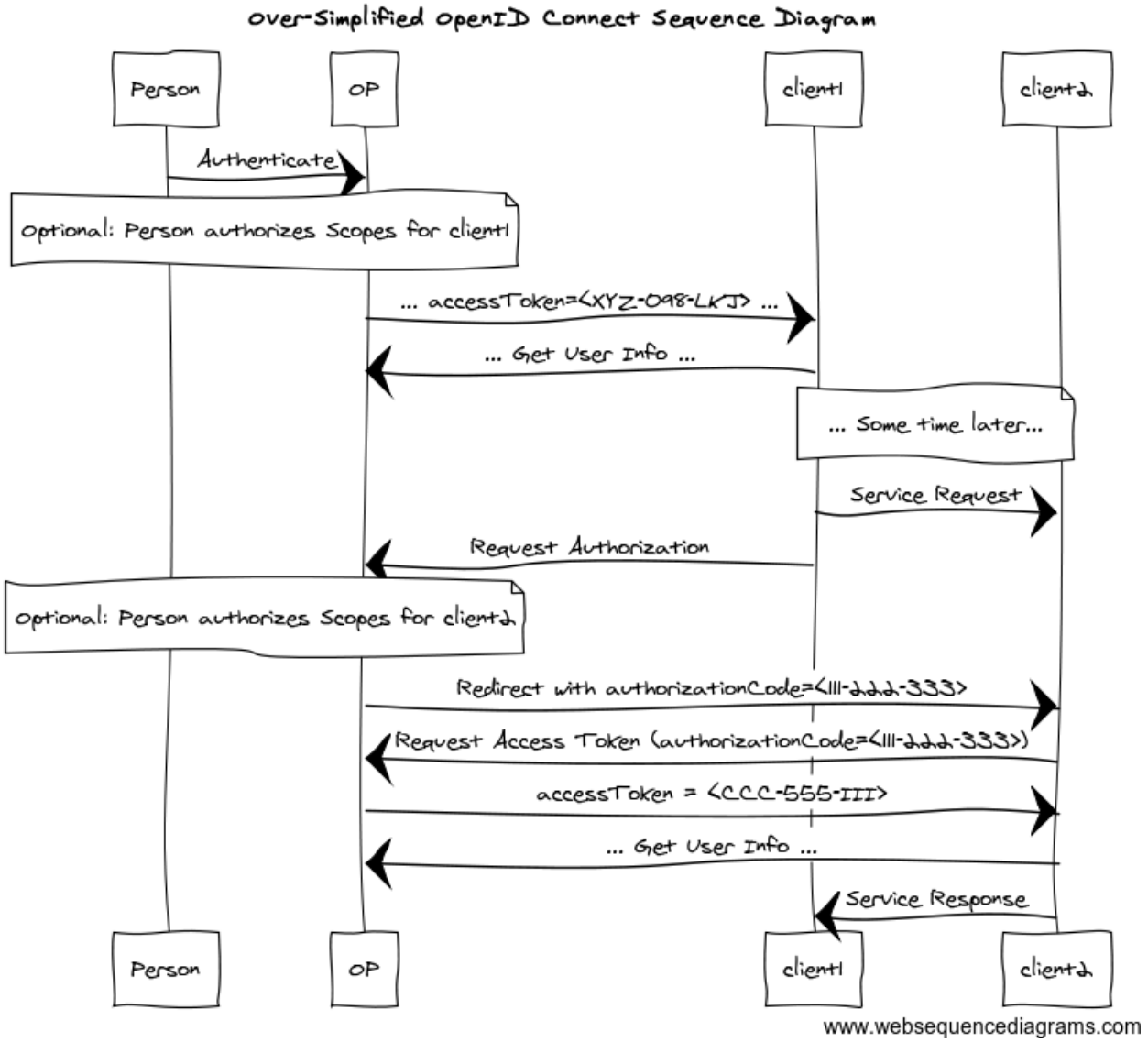
25 May 2012

OpenID Connect Protocol Suite

http://openid.net/connect



gluu


over-Simplified openID Connect Sequence Diagram
Person
OP
client1
client2
Authenticate
optional: Person authorizes Scopes for client1
... accessToken=<XYZ-098-LKJ> ...
... Get User Info ...
... Some time later...
Service Request
Request Authorization
optional: Person authorizes Scopes for client2
Redirect with authorizationCode=<111-222-333>
Request Access Token (authorizationCode=<111-222-333>)
accessToken = <CCC-555-III>
... Get User Info ...
Service Response
Person
OP
client1
client2
www.websequencediagrams.com

Subtle Revolutions

- “SMTP-stlye” email address are the entity identifiers
- Ease of use for Web Developers
- Good usability for People

When ?

- Consumer IDP support 2013
  - Google launch of Account Chooser
- Large websites will support first … 2013
- CMS, CRM, communication and SaaS apps to follow

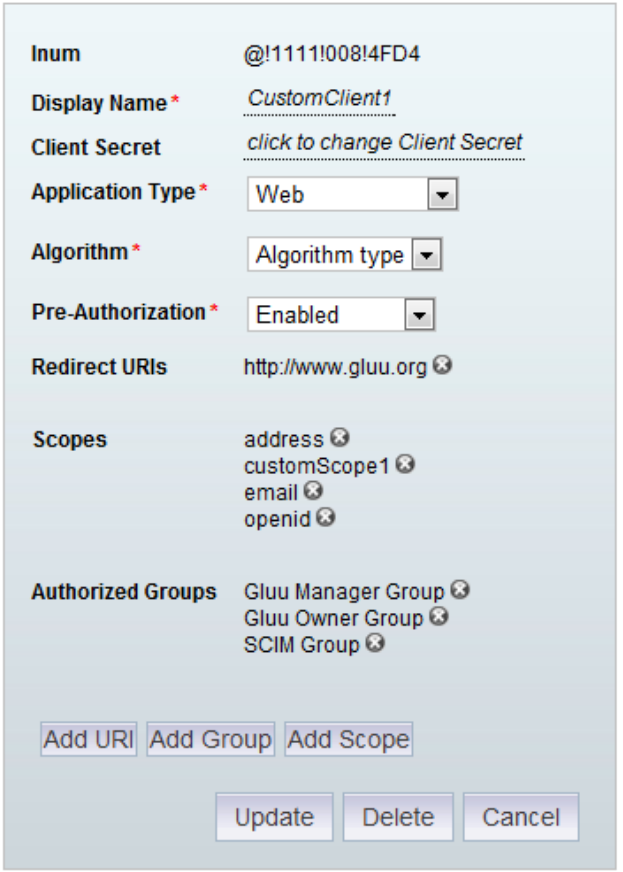
What is next?

Tools and Rules

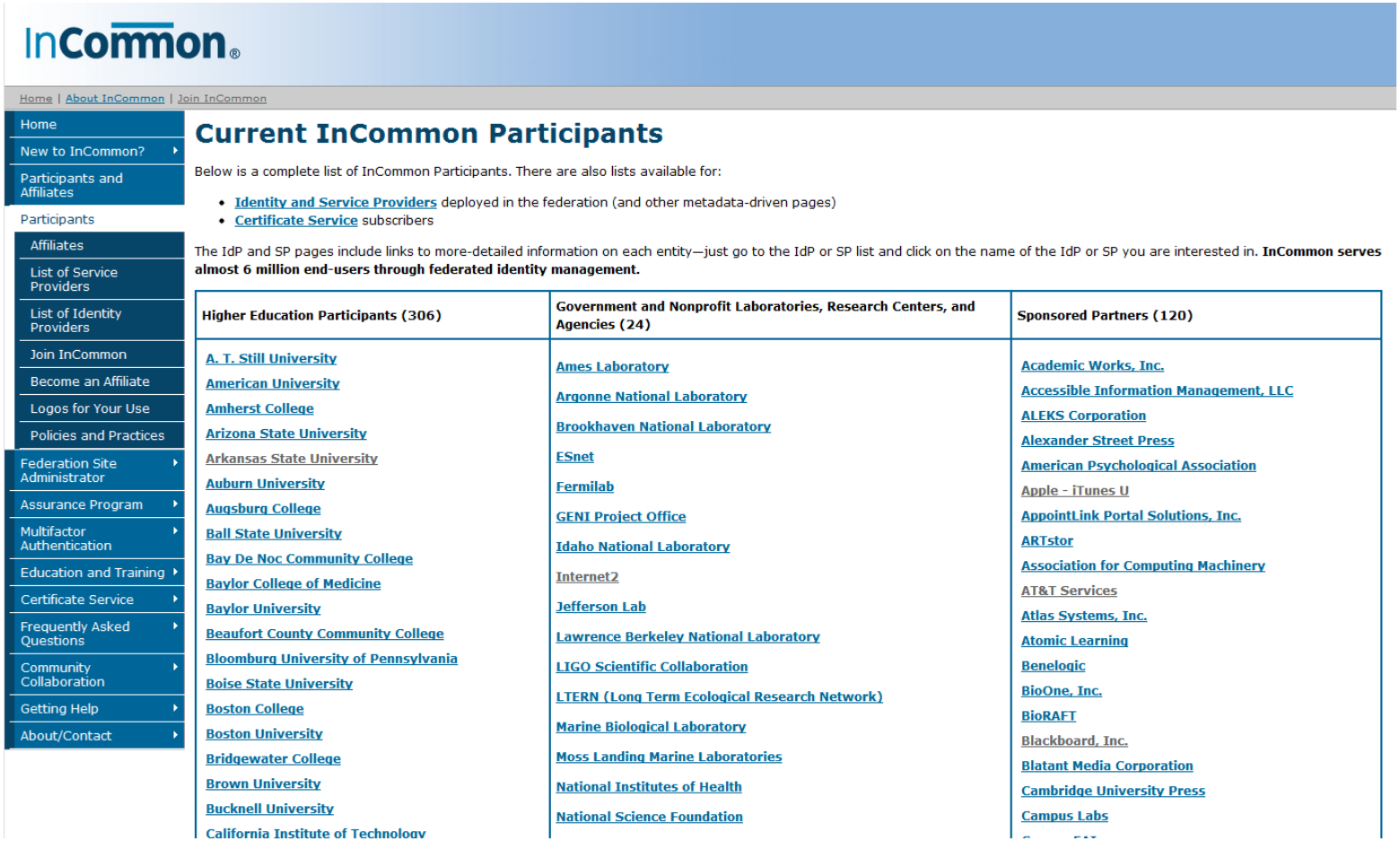
- Tools
  - Its not just the Web, but the depth of software tools and support that makes it so powerful.
- Rules
  - How the standards are used can be strengthened by the central authorities.
  - Both are needed… but rules may take a while

Organizational Trust Management

- Organizational Trust Management
  - Which “clients” are authorized for which scopes?
  - Which people are authorized to use which clients?
  - How to group related clients?



MultiParty Federations In OpenID Connect ?



InCommon®

Home | About InCommon | Join InCommon

- Home
- New to InCommon?
- Participants and Affiliates
- Participants
  - Affiliates
  - List of Service Providers
  - List of Identity Providers
  - Join InCommon
  - Become an Affiliate
  - Logos for Your Use
  - Policies and Practices
- Federation Site Administrator
- Assurance Program
- Multifactor Authentication
- Education and Training
- Certificate Service
- Frequently Asked Questions
- Community Collaboration
- Getting Help
- About/Contact

Current InCommon Participants

Below is a complete list of InCommon Participants. There are also lists available for:

- Identity and Service Providers deployed in the federation (and other metadata-driven pages)
- Certificate Service subscribers

The IdP and SP pages include links to more-detailed information on each entity—just go to the IdP or SP list and click on the name of the IdP or SP you are interested in. **InCommon serves almost 6 million end-users through federated identity management.**

Higher Education Participants (306)	Government and Nonprofit Laboratories, Research Centers, and Agencies (24)	Sponsored Partners (120)
A. T. Still University	Ames Laboratory	Academic Works, Inc.
American University	Argonne National Laboratory	Accessible Information Management, LLC
Amherst College	Brookhaven National Laboratory	ALEKS Corporation
Arizona State University	ESnet	Alexander Street Press
Arkansas State University	Fermilab	American Psychological Association
Auburn University	GENI Project Office	Apple - iTunes U
Augsburg College	Idaho National Laboratory	AppointLink Portal Solutions, Inc.
Ball State University	Internet2	ARTstor
Bay De Noc Community College	Jefferson Lab	Association for Computing Machinery
Baylor College of Medicine	Lawrence Berkeley National Laboratory	AT&T Services
Baylor University	LIGO Scientific Collaboration	Atlas Systems, Inc.
Beaufort County Community College	LTERN (Long Term Ecological Research Network)	Atomic Learning
Bloomburg University of Pennsylvania	Marine Biological Laboratory	Benelogic
Boise State University	Moss Landing Marine Laboratories	BioOne, Inc.
Boston College	National Institutes of Health	BioRAFT
Boston University	National Science Foundation	Blackboard, Inc.
Bridgewater College		Blatant Media Corporation
Brown University		Cambridge University Press
Bucknell University		Campus Labs
California Institute of Technology		

gluu

$1.8 Million NSTIC Grant http://www.nist.gov/itl/nstic-092012.cfm

User Trust Management

- UMA : User Managed Authorization
  - Proposed IETF standard
  - Enable users to centrally store permissions given to applications
  - Also Profile of OAuth2
  - Central “Authorization Manager” infrastructure
  - Specify which Clients have access to which resources (URLs)
  - PEP / PDP architecture
  - Course-grain authentication

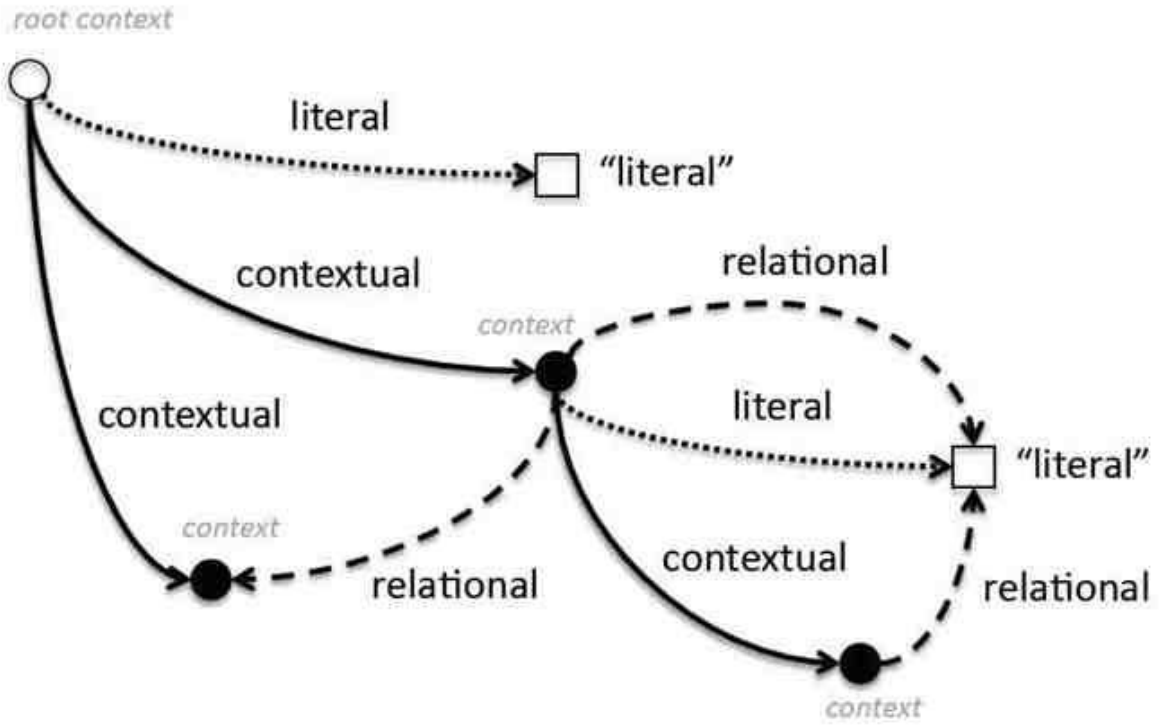
Fine Grain Authorization

- How to specify access to resources
  - Resources need to be described by rules
    - All the pictures in this folder, except these three…
  - Specifying “who” is authorized also needs rules
    - Any teacher in my child’s school can send her a message
    - Note who could also be an organization, federation or some other entity.
  - External conditions
    - During business hours allow hosts from subnet 10.10.10.x
- Many believe to solve this, we need a “Graph” standard

gluu

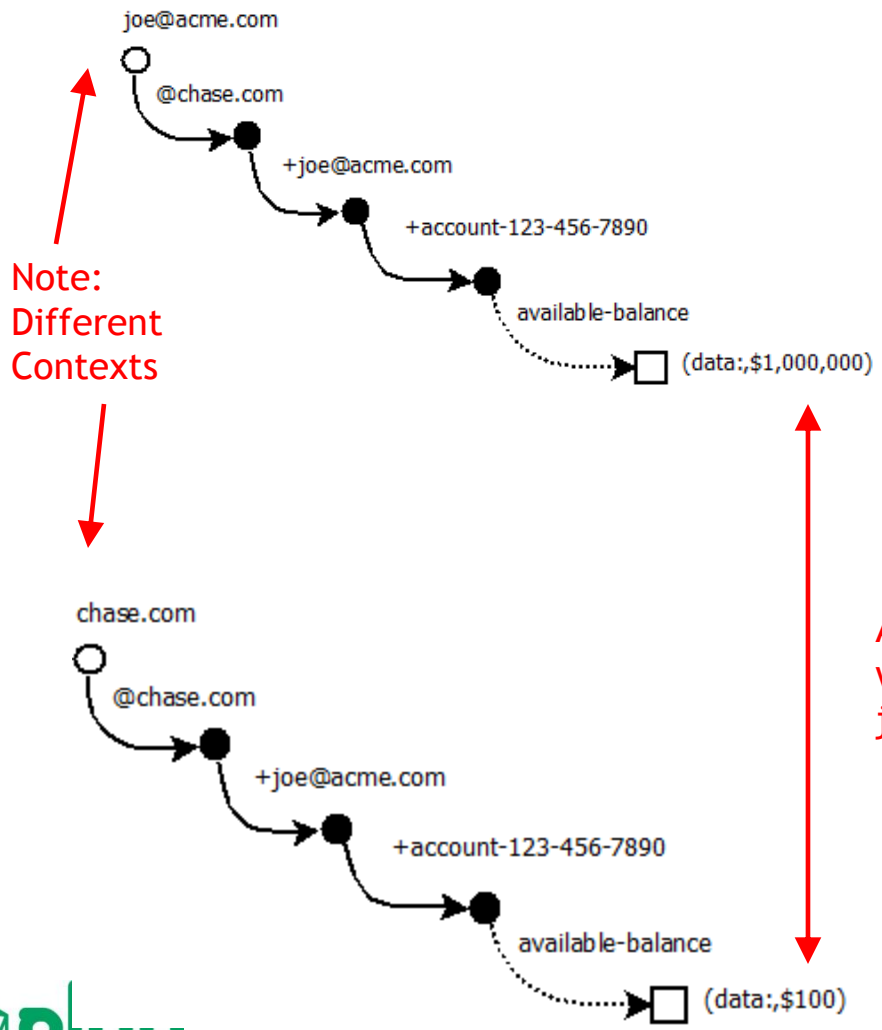
What would an OpenID Graph look like?

There are three types of arcs and nodes: contextual, relational, literal



gluu

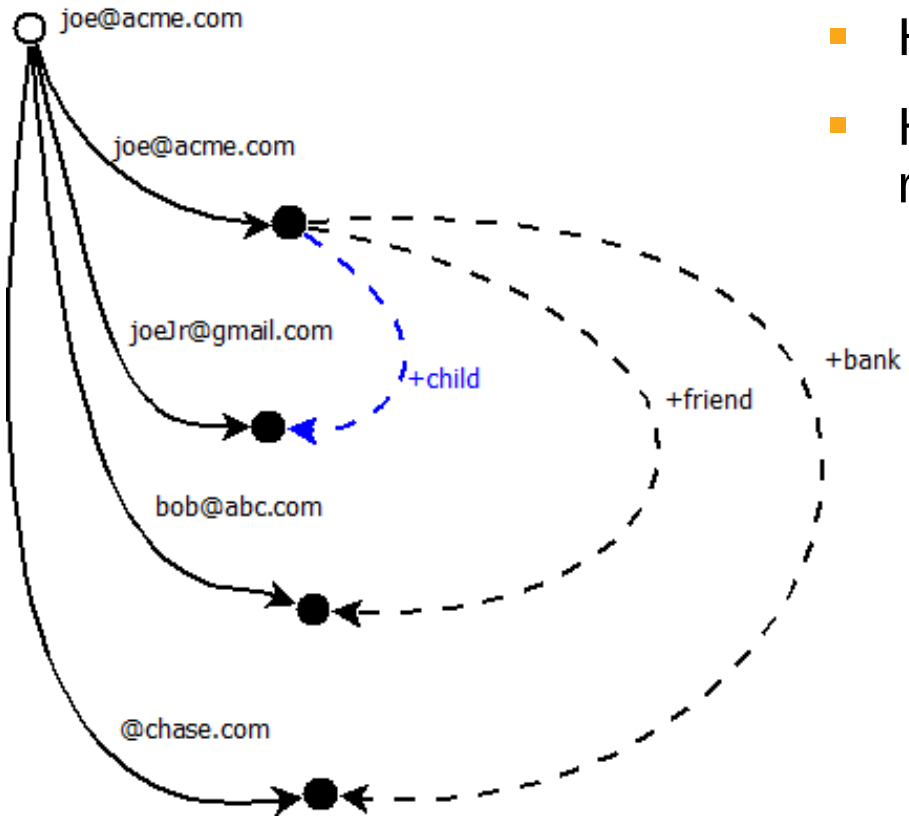
Graph : Contextual Arcs



- What is the provenance of data?
- How to group / organize data

Address of the data is the same, but who are you going to believe? joe@acme.com or chase.com ?

Graph: Relational Arcs

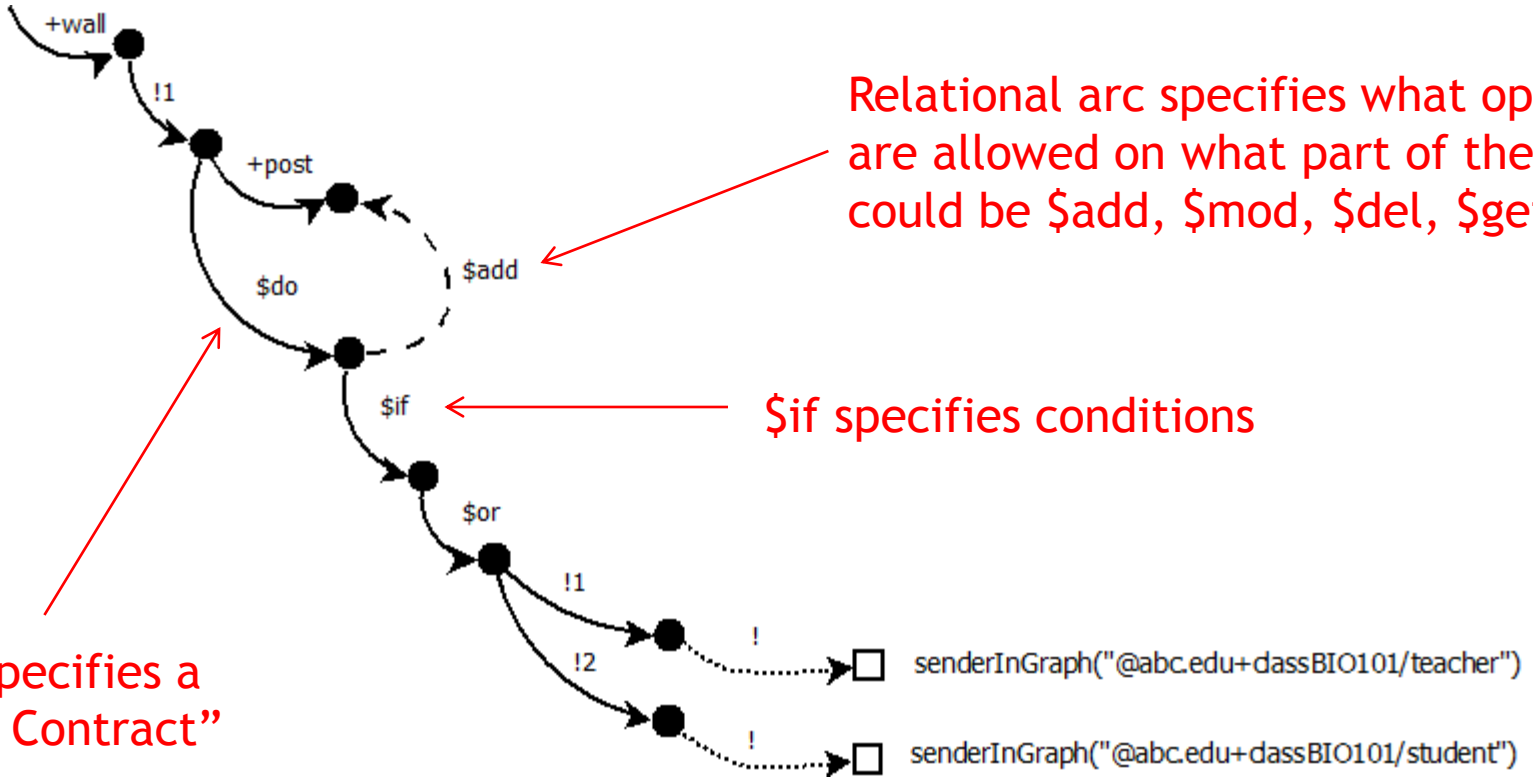


- How are OpenID endpoints related?
- How do we convey real world relationships in the online world?

gluu

Graph: Permissions

(1) What part of the graph (2) what operations (3) under what conditions



Relational arc specifies what operations are allowed on what part of the graph: could be $add, $mod, $del, $get, $all

$if specifies conditions

$do specifies a "Link Contract"

Javascript equation format

gluu

Conclusion

How can you prepare for OpenID Connect?

- If you are a CTO / CSO
  - Deploy an “OpenID Provider” at your organization to enable developers for testing of new applications and cloud service providers.
  - Inquire about the roadmap for OpenID Connect support from your current SaaS providers
  - Define the vision to use OpenID Connect for internal and external SSO
  - Make plans to consolidate existing SAML and SSO infrastructures

How can you prepare for OpenID Connect?

- If you are a Website or App developer
  - Don’t create any more user databases
  - Authenticated via OpenID Connect
  - Use the “User Info” endpoint to request the OpenID Scopes which contain information about the entity.
  - Allow people to identify themselves with an email address: support OpenID Connect discovery.
  - Support OpenID Connect Dynamic Client Registration for your app

How can you prepare for OpenID Connect?

- If you are a Person !
  - Understand that you may need to choose your identity depending on the app or website in question
  - Gripe to websites that don't support OpenID Connect

If you want Open Source OpenID Connect…

- Please checkout the OX project
  - OpenID Connect
  - UMA
  - SCIM
  - OpenID Graph

http://ox.gluu.org

gluu