ESnet
Energy Sciences Network

Identity Ecosystem for Scientific Collaboration

and some related thoughts

Michael Helm

on behalf of Jim Basney, Greg Bell, Irwin Gaines,
Dhiva Muruganantham, Ruth Pordes

http://goo.gl/lZYMU

U.S. DEPARTMENT OF ENERGY
Office of Science

BERKELEY LAB

3 - 5 year outlook

What should OSG, ESnet (and other partners) do to make identity and related protocols work in scientific research partnerships?

Where is research "culture" going?

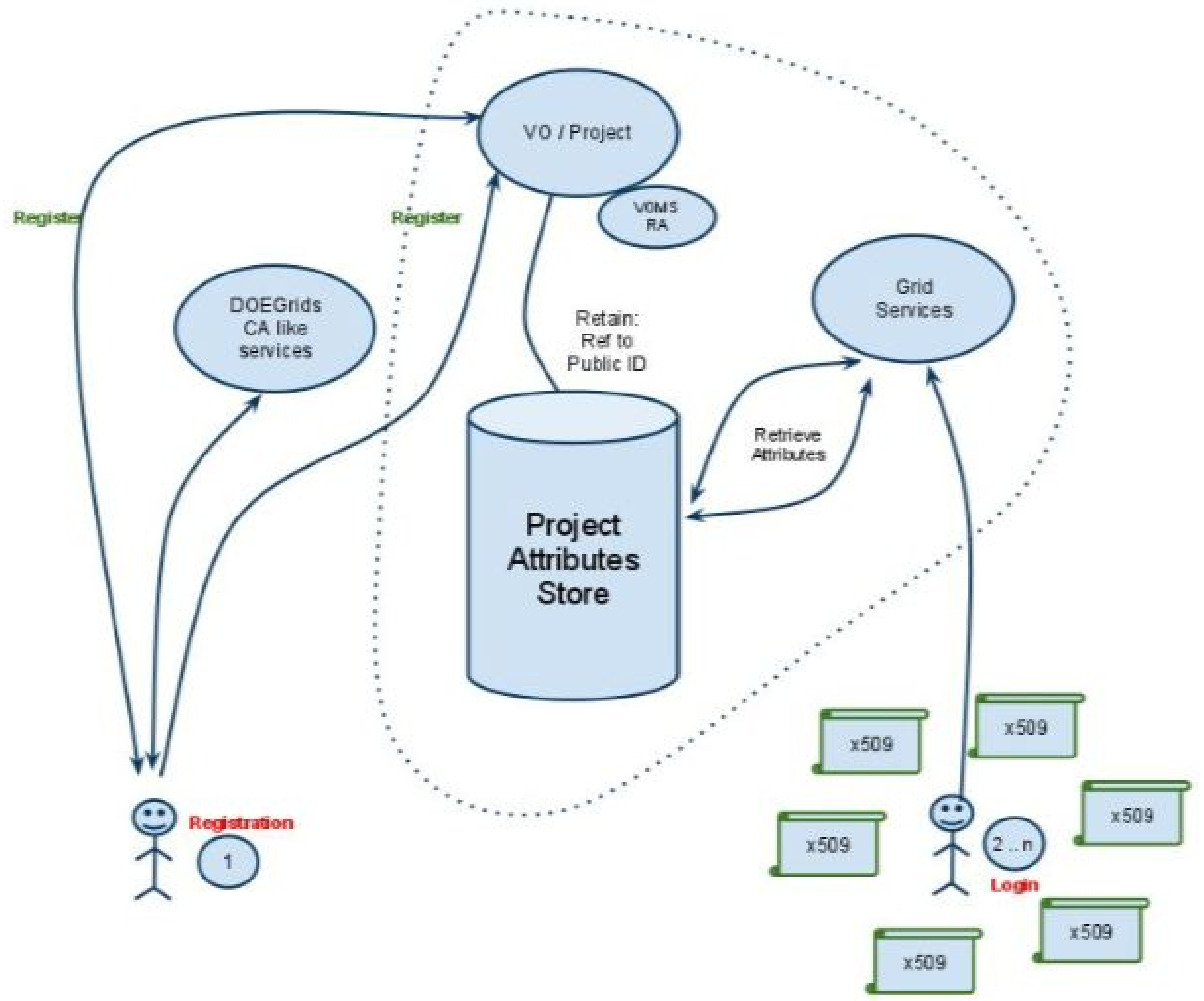
Where is technology and commercial IT headed?

What about PKI?

Scope

- OSG – ESnet document
  - Looking for feedback/critical review of this preview
- Some other things
  - Science Identity Federation (SIF)
  - SAML-Social gateways
  - Mobile
  - The Luddite Position!

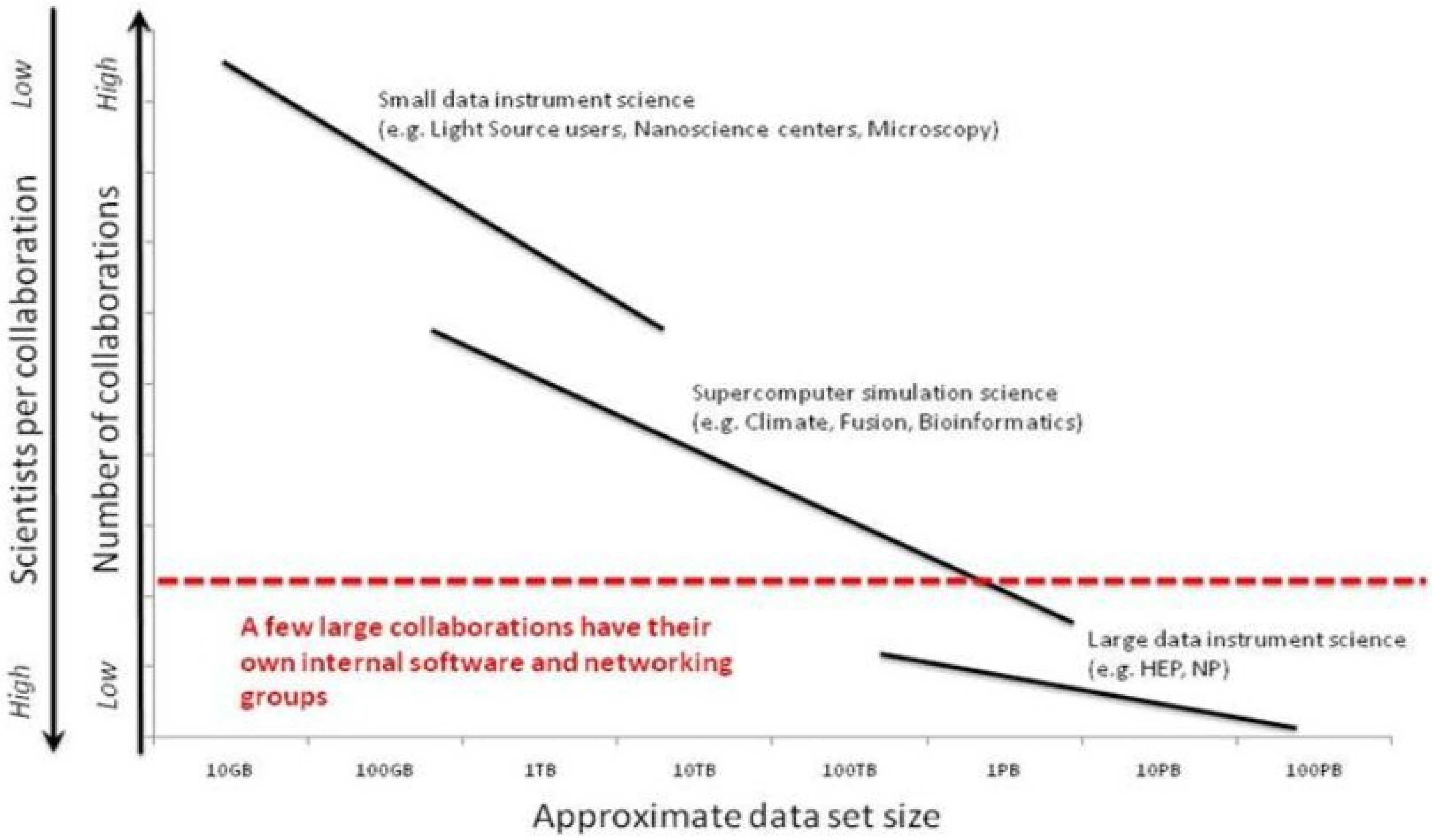
Grids: Combined OSG & ESnet process



The Sociology of Scientific Collaborations

Rough User Grouping By Data Set Size

Courtesy: Eli Dart, ESnet



What do we learn from this?

- Our identity process is a mess
  - Evolved (only partly designed)
  - Nobody is satisfied
  - Inefficient
- Different collaborations have different strengths/weaknesses, requirements, desires
  - Resource constraints
  - Ability to absorb change

OSG-ESnet vision

- NSTIC: use a standard identity proofing framework
- Use authenticators (tokens) from standard ID proofing (where possible)
- Eliminate multiple registrations
- Credential store in the cloud (where PKI goes)
- DNSSEC/DANE for PKI certificates
- Focus on SAML groupware
- OAuth/OpenID Connect for cloud

NSTIC

- Use standard, accredited ID providers
- We *must* have something that is understood outside US borders
- Lower the high cost of federation

Tokens

- Use high quality authenticators (tokens) from standardized ID process
  - Eliminates duplicate services
  - Eliminates user confusion
- Not always possible

Duplicate Registrations

- This is really “project identity” under cover
- We have no choice but to support this pattern as best we can
- Integrate the project “provisioning” process with standardized identity proofing

Keys in the Cloud

- Where are my credentials/tokens !!?!?!?
- We need “follow-me” credentials
- PKI
- OAuth tokens
- Other derived credentials

DNSSEC - DANE

- PKI re-generation
- Disruptive development
  - End of 3rd party PKI business
  - Federation metadata
  - Significant change in DNS operation
- Other offshoots likely
  - CAA – what CAs are authorized for this domain (PKIX)

SAML

- Extensive use of SAML assertions/payloads inside OSG authorization services
- SAML IDPs in use in US Universities … and some national labs (see SIF, below)
- Support from I2/NSF for continued development of groupware tools
- Deepen this investment!

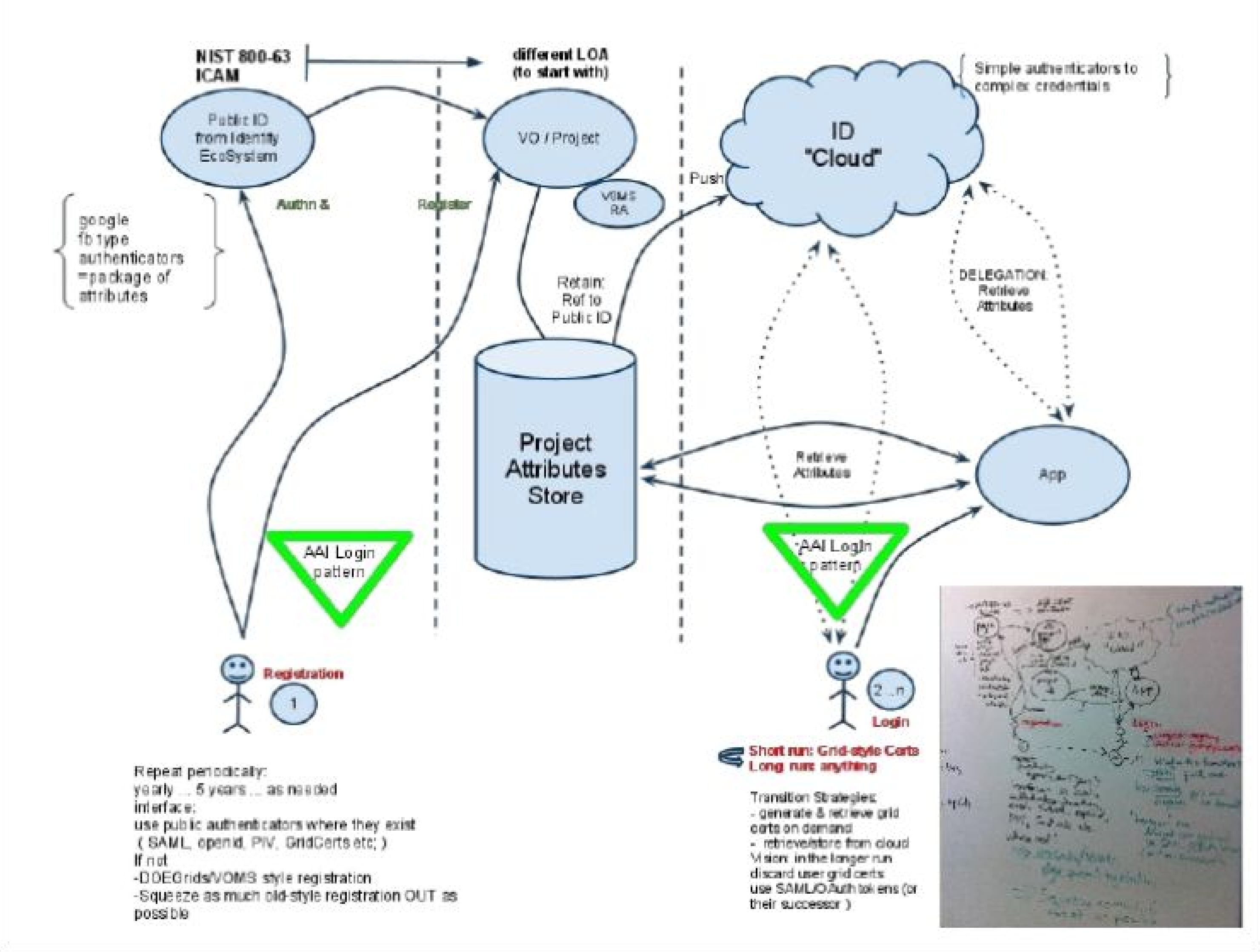
OpenID Connect

- Industry-supported rework of OAuth 2 & OpenID 2
- OAuth 2 – “quantized authorization”
  - OAuth: breakthrough in authZ/delegation without entanglement in identity
- OpenID 2 – “quantized identity”
- Depends on TLS for integrity & confidentiality (see DNSSEC above)
- Like Facebook Connect, but … more open

OpenID Connect (2)

- Basic OAuth flow: App #1 calls App #2 – needs authorization– redirect to OAuth authorization server
  - Gets authorization token for App #2
  - How? User did it directly; pre-authorized; other
- But that’s not enough! Who/what are you?
  - Add User’s OpenID server (OP) as scope
  - Authorized to connect to OP
    - This step “introduces” OP – *connect*
  - Fetch user attributes
- This scenario models our Grid system … maybe
- Cloud providers ... definitely
- RESTful, no SOAP

What will this look like?



Short run: Grid-style Certs
Long run: anything

Repeat periodically:
yearly ... 5 years ... as needed
interface:
use public authenticators where they exist
(SAML, openid, PIV, GridCerts etc;)
If not
-DOEGrids/VOMS style registration
-Squeeze as much old-style registration OUT as
possible

Transition Strategies:
- generate & retrieve grid
certs on demand
- retrieve/store from cloud
Vision: in the longer run
discard user grid certs
use SAML/OAuth tokens (or
their successor)

Science Identity Federation

- DOE Labs collaborate heavily with Higher Ed
- SAML authentication is the best choice
  - For internal, security-related reasons
  - For collaboration with major research universities
  - For international collaborations (inter-federation)
- SIF began at NLIT in 2009
  - We have about ½ of the SC Labs in InCommon
  - We have about ½ of the SC labs with production IDPs
  - The overlap is exactly 2 sites!

SAML – Social Gateways

- Doppelgänger of OpenID Connect
- Gateway between SAML & public resources
  - Facebook, Twitter, Google, &al
  - Map an OpenID attribute into a SAML assertion for local consumption
- In the long run, the co-evolution of OpenID Connect and SAML federation

Mobility/Mobile computing

- Can the disruptive effect of mobile computing be overestimated? I don’t think so.
- We can expect
  - Different authentication techniques
  - Need for application access on mobile device or
  - Applications executing directly on mobile device
  - Further erosion of heavy-weight web protocols
  - Network effects

Not everybody is eager!

The Conservative Position

Some things I hear….

- We’re doing real work here
- We mix command line & web tools
- We don’t collaborate at the major institute level
- We collaborate at
  - The individual level
  - The department/small lab/company level
  - Our “collaborators” are “competitors”

One position in particular….

- We are happy, & think it’s appropriate, to be the **gatekeeper** to the ID token issuance process
- We do want the processes & roles around it to improve
- We want to delegate the group membership and manage this process
- We want to be part of the policy process, & participate in the technical infrastructure that manages it
- We’re happy to use technology to support this (eg SAML, OpenID) but replace it

This is not a Luddite position!

- We can develop and improve our identity infrastructure …
- As long as we listen to, respect, and adapt to requirements and patterns we find, including this one

Outlook

- Don’t be confused! We can get value from *all* of these technologies now.
- Opportunity: more local control, decentralization (= federation, but more evolved)
- Opportunity: increased efficiency & reduced friction – need small R&D effort to move forward
- Lesson from Google - where is our market research?