Update on Internet Identity and Scalable Access Control

Ken Klingenstein, kjk@internet2.edu

Topics

- Identity
  - Federal update
  - InCommon and eduGAIN
  - Social2SAML gateways and IdPoLR
  - Federated incident handling
  - ORCID identifiers
- Access control
  - RD-Alliance and related observations
  - Attribute-based access control
  - Attribute release and consent management
  - VO Collaboration software
- Futures
  - Vectors of trust
  - Using federation to distribute other sources of authority

Federal initiatives

- FICAM
- NSTIC
- The Snowden effect
  - On standards
  - On internal federal approaches

FICAM

- Federal operational authentication+ service
  - Agencies to agencies, citizens, businesses
  - The current incarnation of 20 years of federal efforts
    - Includes the federal PKI Bridge that still provides effective if limited services
    - Includes connect.gov, the citizen and enterprise portal
    - InCommon can provide LOA 1 and 2 IdPs
- Challenging work
  - Certifying IdP's is not yet a marketplace
    - See Kantara
  - Agency incentives for change are limited
  - Big social IdP's set their own rules

INTERNET 2

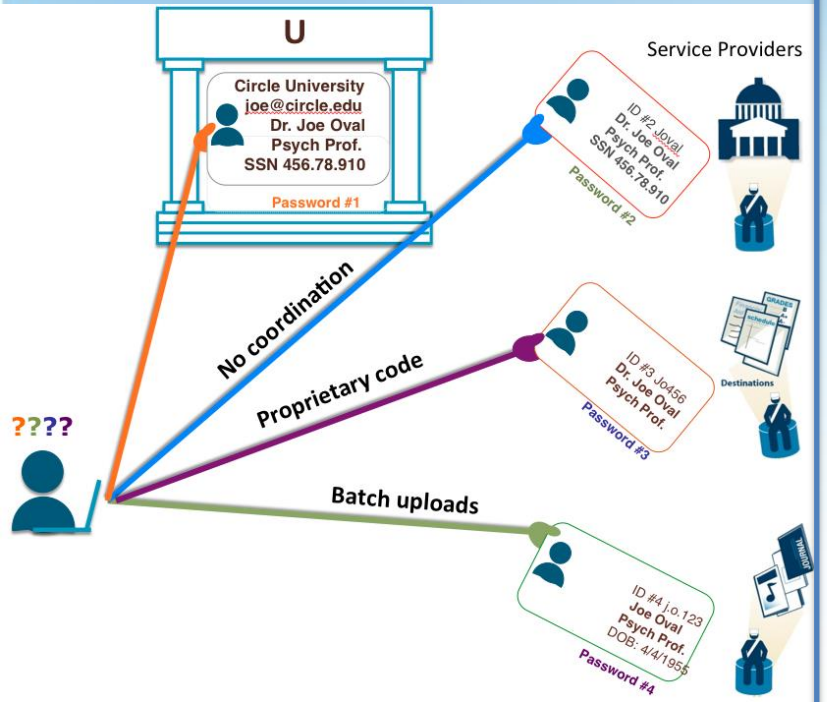
NSTIC

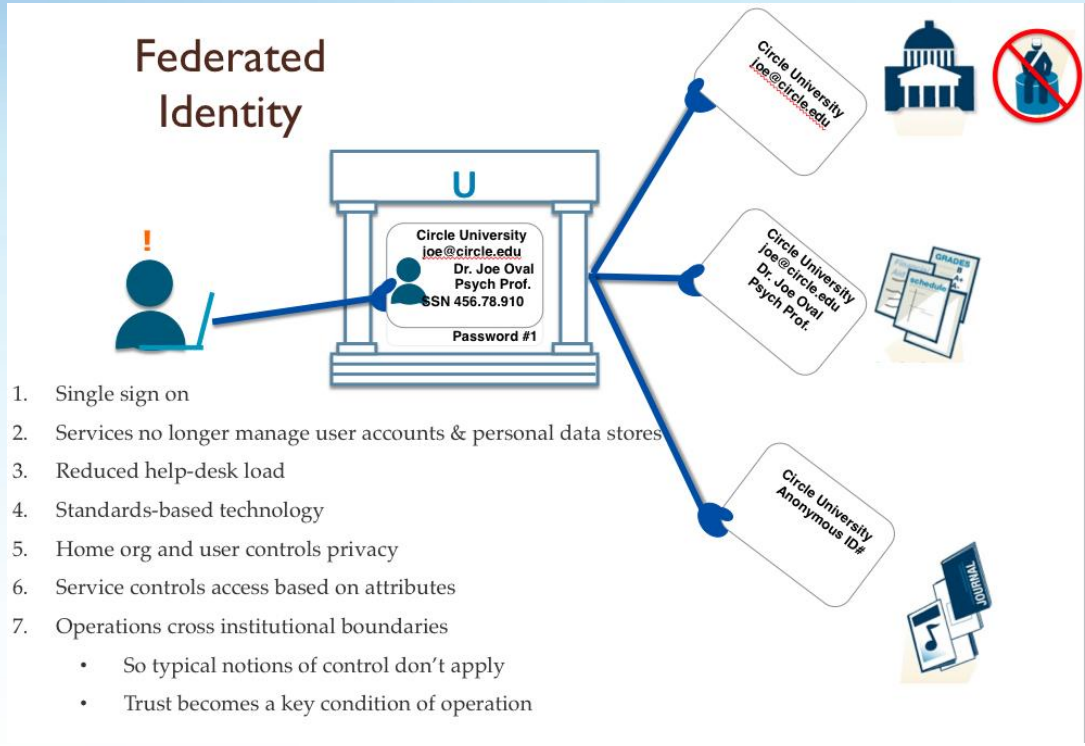
- Created by Obama, operated out of Commerce and NIST
- Broader scope, more developmental
- Has two dimensions:
  - Governance, called IDESG, (idecosystem.org), now a 501c3, intended to set the rules of the road for privacy, security, interoperability, etc..
  - Pilots funded for 2-3 years, spanning start-ups, infrastructure builders, trust mechanisms, federated incident handling

    Also informs governance
- Private/public partnerships, especially around difficult issues such as privacy and trust, are hard.

INTERNET 2

Federated Identity & Access Management





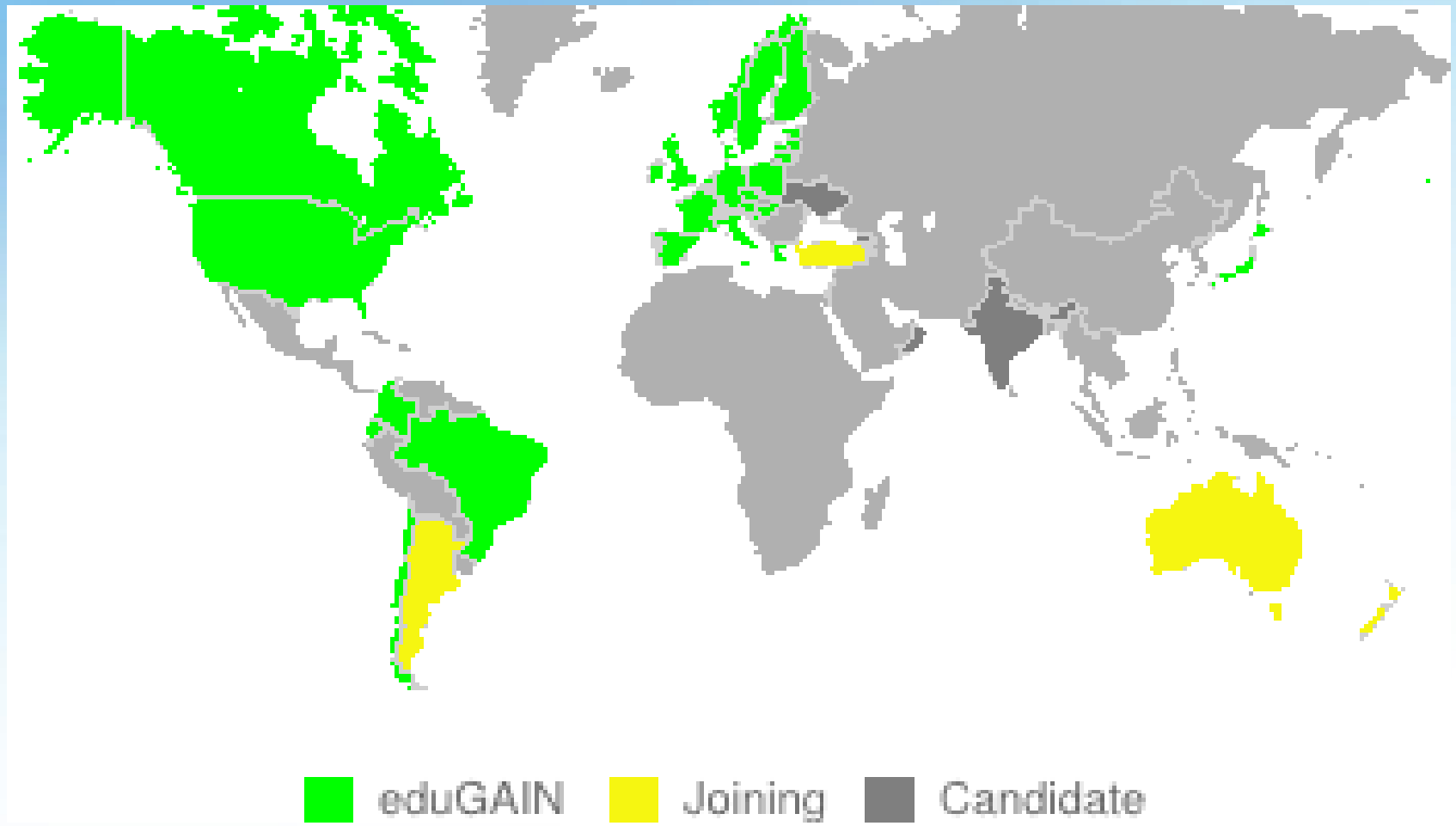
1. Single sign on
2. Services no longer manage user accounts & personal data stores
3. Reduced help-desk load
4. Standards-based technology
5. Home org and user controls privacy
6. Service controls access based on attributes
7. Operations cross institutional boundaries
   - So typical notions of control don't apply
   - Trust becomes a key condition of operation

INTERNET 2

InCommon

- 700 + participants, essentially all academic research institutions
- Hundreds of service providers, from Azure to AWS, Elsevier and IEEE, Microsoft to Box, Argonne to Pacific Northwest Labs to Woods Hole
- Certificate services important; MFA devices and licenses growing value
- MFA use on campuses is increasing significantly
- Metrics need to change from number of participants to intensity of participation per member
  - Single biggest challenge is attribute release

Edugain membership



InCommon and eduGAIN

- InCommon has joined eduGAIN
  - Has a metadata service ingestion mechanism being tested
    - Starting dynamic metadata testing within InCommon
  - Exporting InCommon metadata into eduGAIN also in the plans
    - First IdP's, then SP's
    - Opt in/out sets of issues
- Exposes the next set of critical issues, some of which are almost showstoppers
  - Attribute release internationally
  - Inconsistent semantics of common attributes

Social2SAML Gateways and IdPoLR

- We make extensive use of Social2SAML gateways
  - Expands user base to students' parents, contractors, alumni, etc..
  - Friendly commercial service works with campuses
  - Exposes next sets of issues – LOA, filtering out attributes, etc.

- IdP of Last Resort (extensions of Commit)
  - Yet another way to serve a broader community that wants into our world
  - Slowly building an IdP to serve college admissions, and likely beyond
  - Business process takes the identities into high assurance
    - MFA
    - Identity vetting at College Testing services

End-entity tags

- Intended to convey information about the end-point to others in the federation
  - Research and Scholarship (R&S)
    - Nature of the application (and required attributes)
    - Willingness of the IdP to release
  - Hide from discovery
    - For IdP's
  - Follows Euro "Code of Conduct"
  - Many, many others to follow
    - Creating "virtual" federations within federations
- Will expose the next set of needs
  - E.g. harmonization of affiliation faculty/student/staff

Federated incident handling

- Concerns of major science service providers that if they go the federated route, they will be notified by IdP's of compromised accounts relevant to the service provider.
- "Sir-T-FI" initiative to define and solve the problem
- Aligns well, surprisingly, with some innovative commercial sector thoughts (see confyrm.com)
- Stay tuned

ORCID identifiers

- Purpose is to provide a unique, persistent, resolvable identifier
  - Primary purpose is disambiguation of scholarly identity, ability for a scholarly identity to claim a set of works and publications
  - To be a part of the ScienCV mechanisms
  - Publishers and agencies help driving
- Business model is “evolving”
  - Free to individuals; enterprises that want to issue bulk can purchase site licenses
- Concerns to be worked on
  - Claiming an ORCID identifier
  - Controlling release of associated information
  - Use for account linking purposes

INTERNET 2

Identity, identifiers and attributes

- Identity is you and your account
- Identifiers are unique values tied to you, but often offering privacy instead of identity
  - Different identifiers give different type of privacy
    - (opaque but stateful, opaque and non-correlating, etc..)
- Attributes provide privacy, access control and scale
  - Attributes fall into two rough categories
    - Verified – by the identity provider, an attribute provider, a third party verifier, etc.. e.g. Legal name, legal date of birth, over legal age, citizenship, student status, role in organization, is in Class X, walk-in-library-user, is PI of a NIH grant in oncology, etc..
    - Self-asserted – e.g. displayname, friends, interests, preferredlanguage and many from that might better be verified

RD-Alliance and related

- RD-Alliance meeting in San Diego
  - Working hard to gain traction, be relevant, not be overtaken by events
  - Dynamic between the elegant and abstract on one hand and the urgent and practical (e.g. open access)
  - Tension between domain use and cross-domain use at core of the challenge
- Large-Scale Projects meet RDA workshop
  - https://rd-alliance.org/large-scale-data-projects-meet-rda-rda-5th-plenary-session.html
- Open Access

INTERNET 2

Large Scale Data Projects

- EPOS: A large scale distributed Heterogeneous Research Infrastructure for GeoScience, Earth System Grid, ELIXIR, DataNet One, Chandra, CLARIN, National Data Service, etc.
- Boots on the ground workers solving a similar set of problems, often in somewhat similar but not interoperable fashion.
- Often unaware of existing infrastructure or tools
- What parts of this ocean to boil and how?
  - Identity
  - Access control
- If the cross-domain is important, then a cross-agency (and intra-agency) effort is needed.
  - Structured and supported mappings

Open Access

- Open Access is not necessarily wide open access
  - Lots of use cases for access getting more open over time
  - Lots of use cases for access being closed but metadata about the data being open
  - Even use cases for virtual reading rooms with no note-taking
- Affects discovery and use
- Open access is also accessible access

INTERNET 2

Use cases and requirements for attribute-based access control

- Student in class Physics 1010
- Extension offices
  - "as a land-grant we must make all content available to anyone who is physically in the Library, regardless of . . ." or
  - " because of ADA, we must make public content not only available but accessible" or
  - or "because of the conditions of a gift on content X, we must make it available only to users in situation Y" or . . .
- Institutional repositories for complex interrealm sharing
- Alumni options for access
- Get rid of IP-address only options
- Research Data

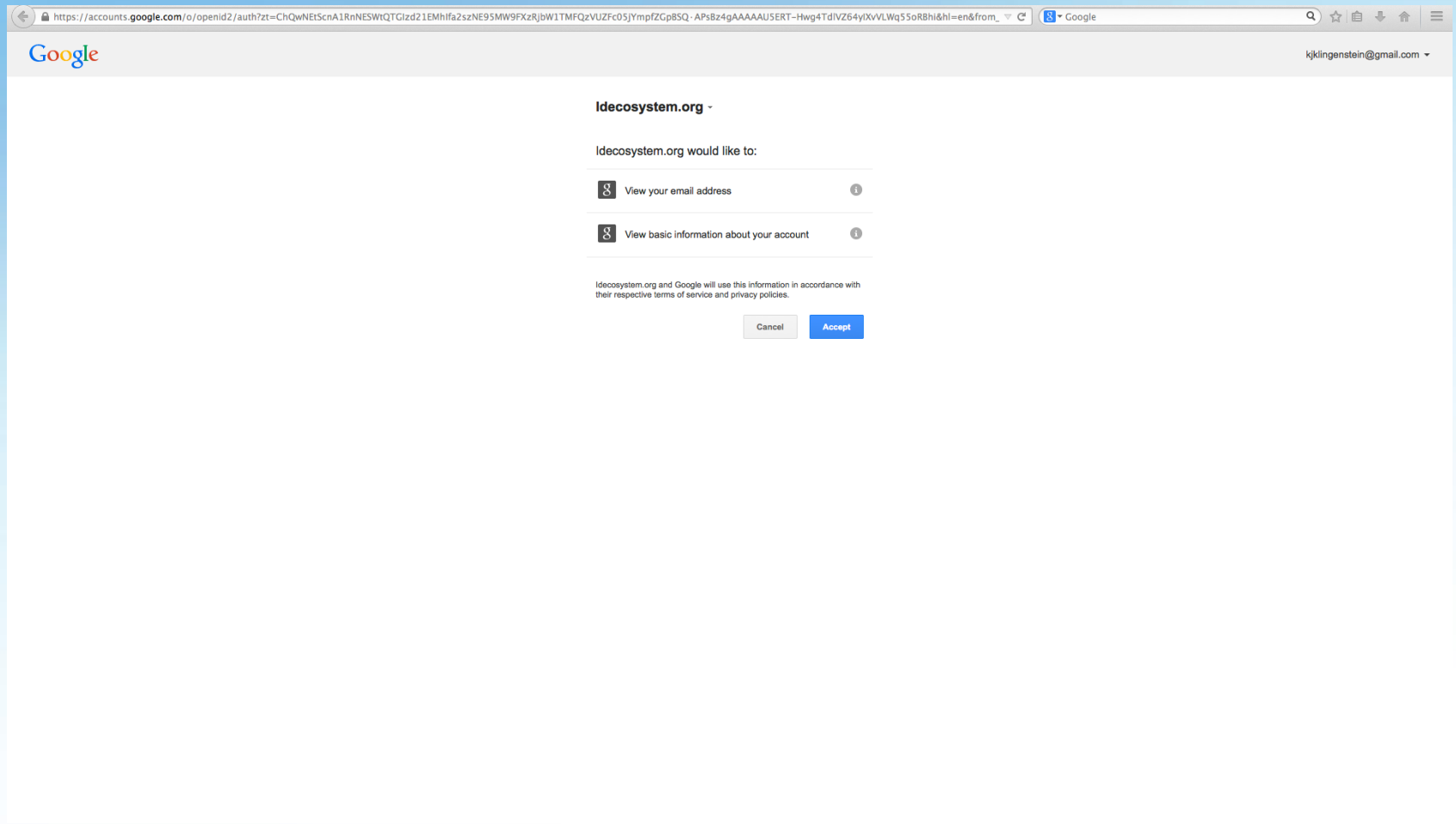
  is PI of a NIH grant in oncology, etc..

  Progressive staged expansion from restricted access

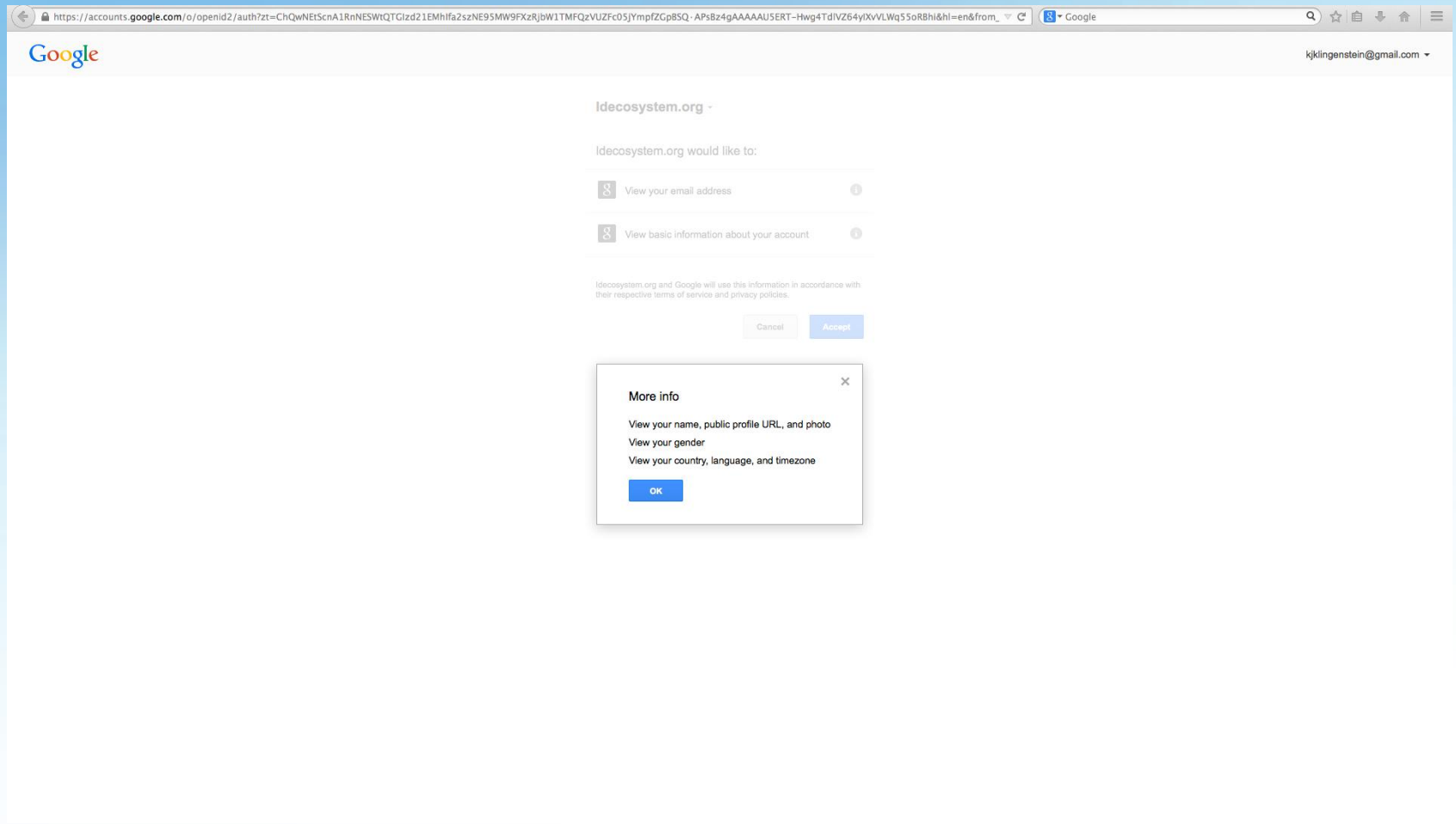
  What to do when the data is open but the tools that access them are copyrighted?

Attribute release and consent management

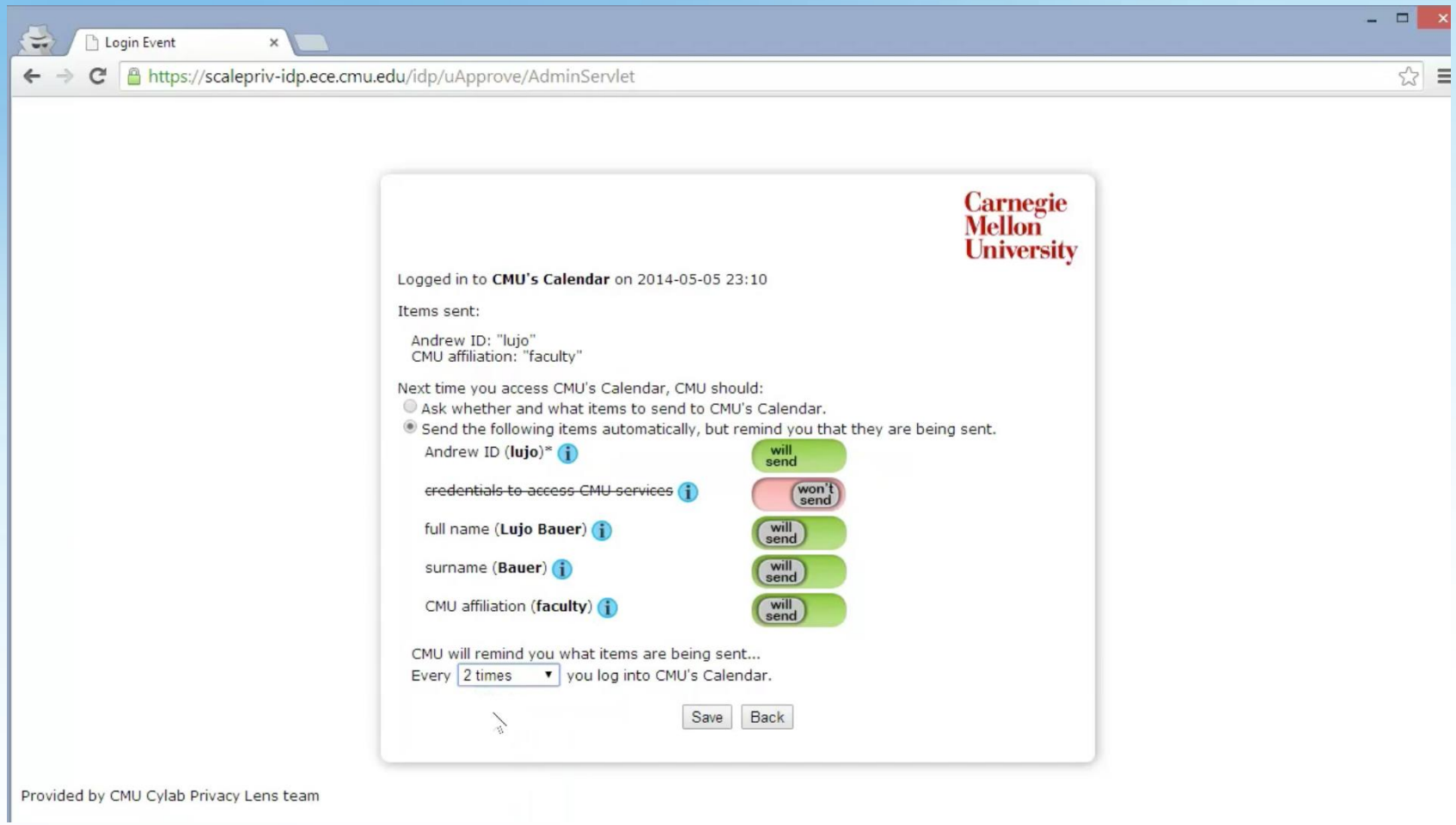
- Attribute release is the single highest barrier to use
- Key dimension of privacy
- Complex set of legal and technical and international and financial and … issues
  - When and where and how to use is endless discussion
  - Initial and downstream are separate but very related topics
- Requirements list grows – informed, revocable, accessible, etc..
- Worst case are medical information
- The capabilities of the end user are limited


https://accounts.google.com/o/openid2/auth?zt=ChQwNEtScnA1RnNESWtQTGIzd21EMhIfa2szNE95MW9FXzRjbW1TMFQzVUZFc05jYmpfZGp8SQ·APs8z4gAAAAU5ERT-Hwg4TdlVZ64ylXvVLWq55oR8hi&hl=en&from_
Google
Google
kjklingenstein@gmail.com
Idecosystem.org
Idecosystem.org would like to:
View your email address
View basic information about your account
Idecosystem.org and Google will use this information in accordance with their respective terms of service and privacy policies.
Cancel
Accept

INTERNET 2


https://accounts.google.com/o/openid2/auth?zt=ChQwNEtScnA1RnNESWtQTGIzd21EMhlfa2szNE95MW9FXzRjbW1TMFQzVUZFc05jYmpfZGp8SQ · APs8z4gAAAAU5ERT-Hwg4TdlVZ64ylXvVLWq55oRBhi&hl=en&from_
Google
kjklingenstein@gmail.com
Idecosystem.org
Idecosystem.org would like to:
View your email address
View basic information about your account
Idecosystem.org and Google will use this information in accordance with their respective terms of service and privacy policies.
Cancel
Accept
More info
View your name, public profile URL, and photo
View your gender
View your country, language, and timezone
OK

PrivacyLens privacy manager



INTERNET 2

PrivacyLens as a paradigm

- Enabling effective and informed end-user consent
- Embraces a set of capabilities
  - Hierarchical information, fine grain control, bundling, revocation of consent, flexible notifications, etc..
- Embraces a style of presentation
  - Clear screens and slides
  - Optional display of values being sent
  - Affirmative user actions
- Embraces a variety of platforms and management approaches
  - Protocol-agnostic
  - Enterprise management consoles and management
  - Audit and security logs

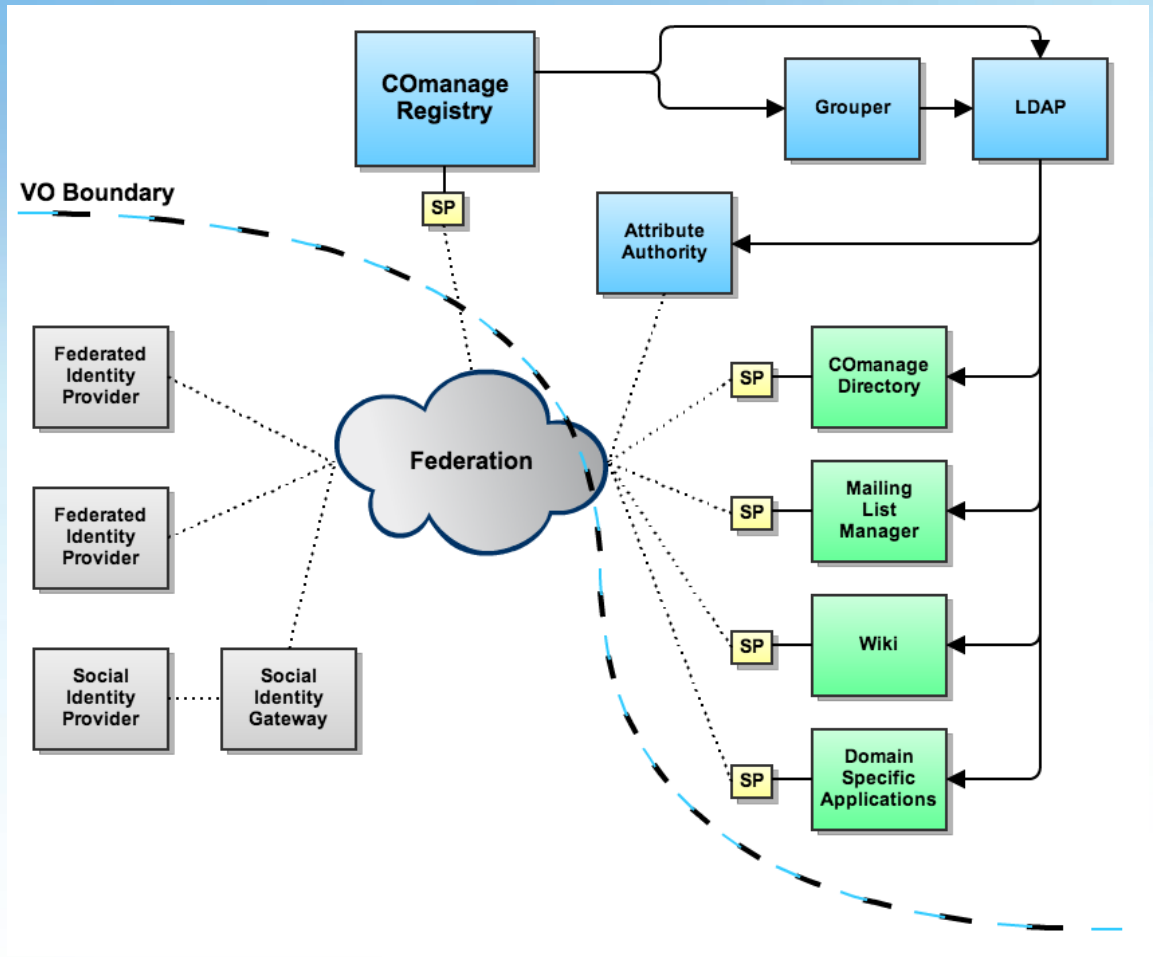
INTERNET 2

VO Support and Collaboration platforms

- The identity landscape is evolving, from authentication (reasonably in hand now) to attributes and access control
- For the R&E community in particular, collaboration platforms are what's important now
  - For enterprises
  - For virtual organizations
- Collaboration platforms integrate federated identity and attributes with local authorization across the set of applications – scientific, collaborative, scholarly, administrative - that a collaboration uses.
- Management of collaboration critical infrastructure, along with instruments, data sets, etc..
- There are more groups than there are identities

INTERNET 2

Management of the collab tools



Approaches to supporting collaborations

- At a national level, e.g. SURFConext, Australia
  - Provides comprehensive federation and collaboration infrastructure to VO's
- At a specific resource or software service
  - E.g. CERN, Globus
- As an open source platform run by a VO
  - LIGO, iPlant
- As an outsourced service offering
  - Multi-messenger astronomy, NIH AIDs

INTERNET 2

Rethinking Vectors of Trust

- NIST 800-63 didn't quite get it right
  - It didn't separate identity proofing from issuing of credential
  - It doesn't handle mobile devices well
  - It doesn't reflect operational security practices outside of identity
    - If you didn't patch Heartbleed , why should I trust your assertion
- Conversations are going on internationally about replacing 800-63
  - It would be good to have it be an international standard

INTERNET 2

Other trust authorities in metadata

- Dynamic metadata is now beginning to be shared among thousands of organizations
- Numerous other trust (but not identity specific) metadata could be shared inexpensively and securely
  - Trusted citations from publishers
  - Trusted provenance authorities sharing their signing keys
  - Custom end-entity tags for discovery purposes
- Leveraging federation business processes to significantly reduce costs