Things Identity:
Federated, Social, Scholarly et al

Topics

- Social identity update
- Federated identity update
  - International
  - InCommon
  - US Government
  - NSTIC grants
- Scalable Privacy activity and its deliverables
- Scholarly identity dimensions
  - CIlogon
  - Eduperson and ORCID
- Collaboration platforms

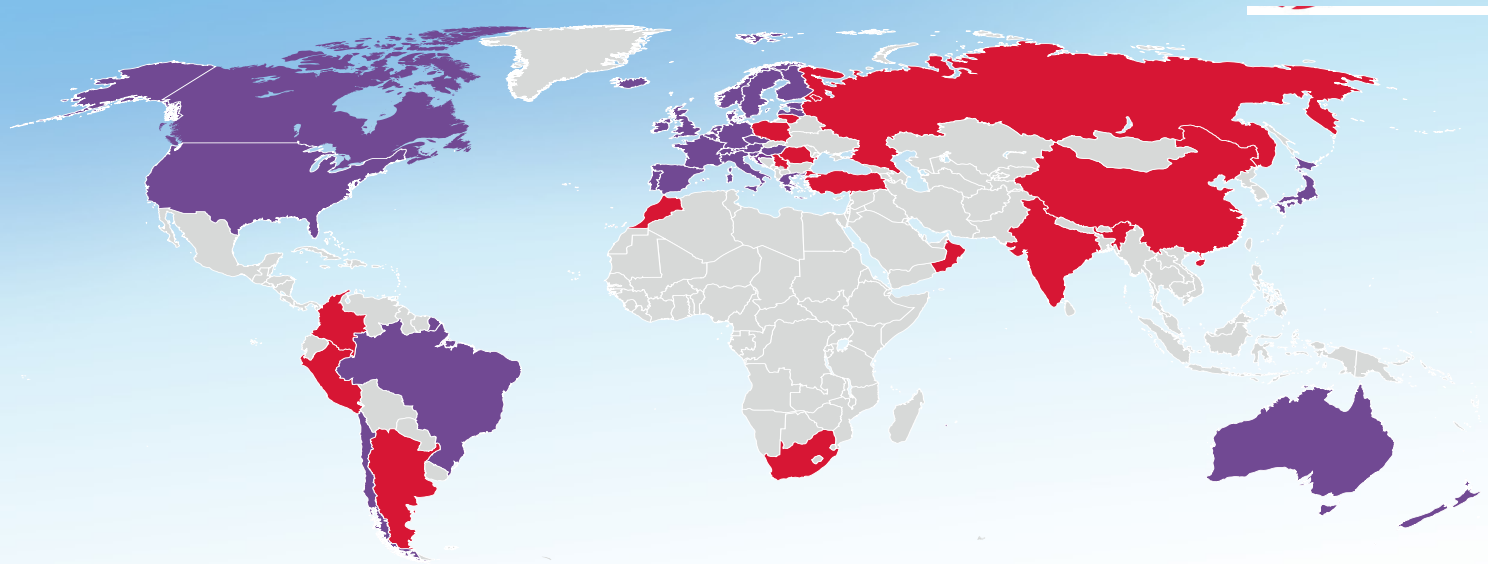
INTERNET 2

Social identity update

- Reaching saturation
- Focus of service to consumer continues on
  - Interest in connecting to federal services unclear
  - T+C's are critical to consumer as a service
- Protocol evolution towards OpenId Connect continues
  - IETF Standards now almost done
  - Many but not all (e.g. Facebook) moving slowly towards standard
  - The value lies in Oauth for mobile app use
- FIDO alliance promoting MFA; identity proofing stays risk-based per RP
- The Yahoo email address persistence policy change opened eyes
- The NSA revelations are changing international marketplaces

INTERNET 2

R&E federations world-wide



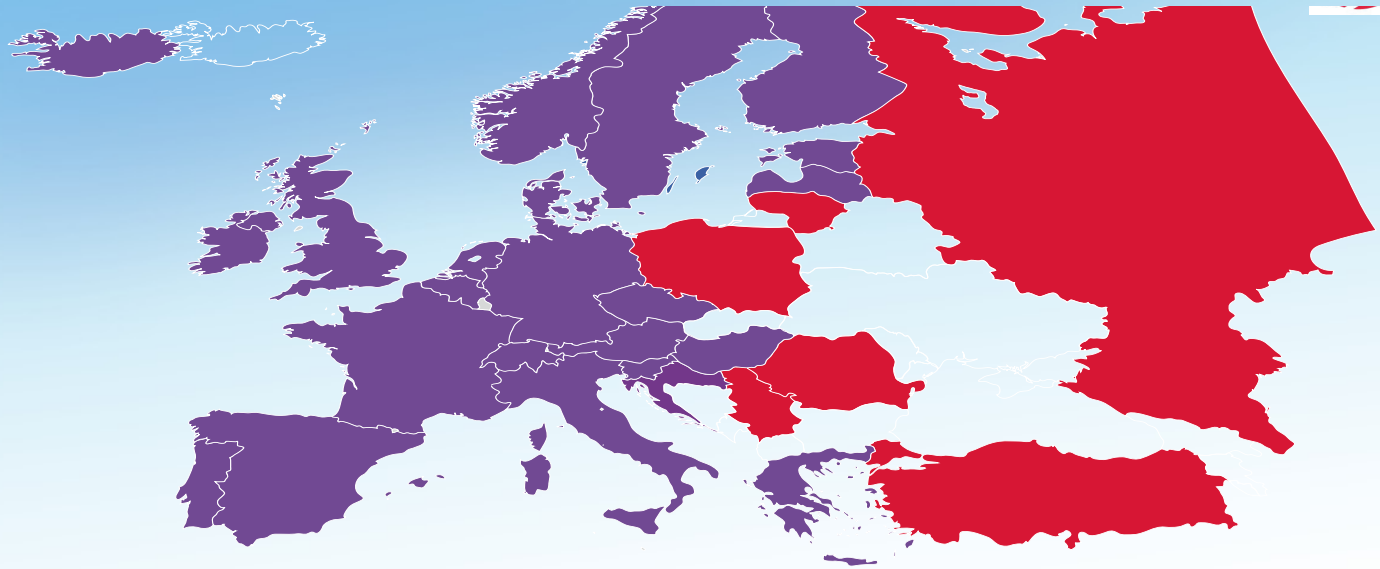
Identity Federations in production

AT	ACOnet Identity Federation	ES	SIR	NL	SURFconext
AU	Australian Access Federation AAF	FI	Haka	NO	FEIDE
BE	Belnet R&E Federation	FR	Fédération Éducation-Recherche	NZ	Tuakiri New Zealand Access Federation
BR	CAFe	GR	GRNET	PT	RCTSaai
CA	Canadian Access Federation CAF	HR	AAI@EduHr	SE	SWAMID
CH	SWITCHaai	HU	eduID.hu	SI	ArnesAAI Slovenska
CL	COFRe	IE	Edugate	UK	UK Access Management Federation for Education and Research
CZ	eduID.cz	IT	IDEM		

Identity Federations in pilot

AR	MATE	PL	PIONIERId
CN	CARSI	RO	RoEduNet Federation
COL	COLFIRE	RS	iAMRES
IN	INFED	RU	ΦEDUrus AAI
LT	LEFT	TR	YETKİM
PE	INCA	ZA	SAIF
MA	eduIDM		
OM	Oman Knowledge ID Federation		

R&E Europe



Identity Federations in production

AT	ACOnet Identity Federation	FI	Haka	NL	SURFconext
BE	Belnet R&E Federation	FR	Fédération Éducation-Recherche	NO	FEIDE
CH	SWITCHaai	GR	GRNET	PT	RCTSaai
CZ	eduID.cz	HR	AAI@EduHr	SE	SWAMID

Identity Federations in pilot

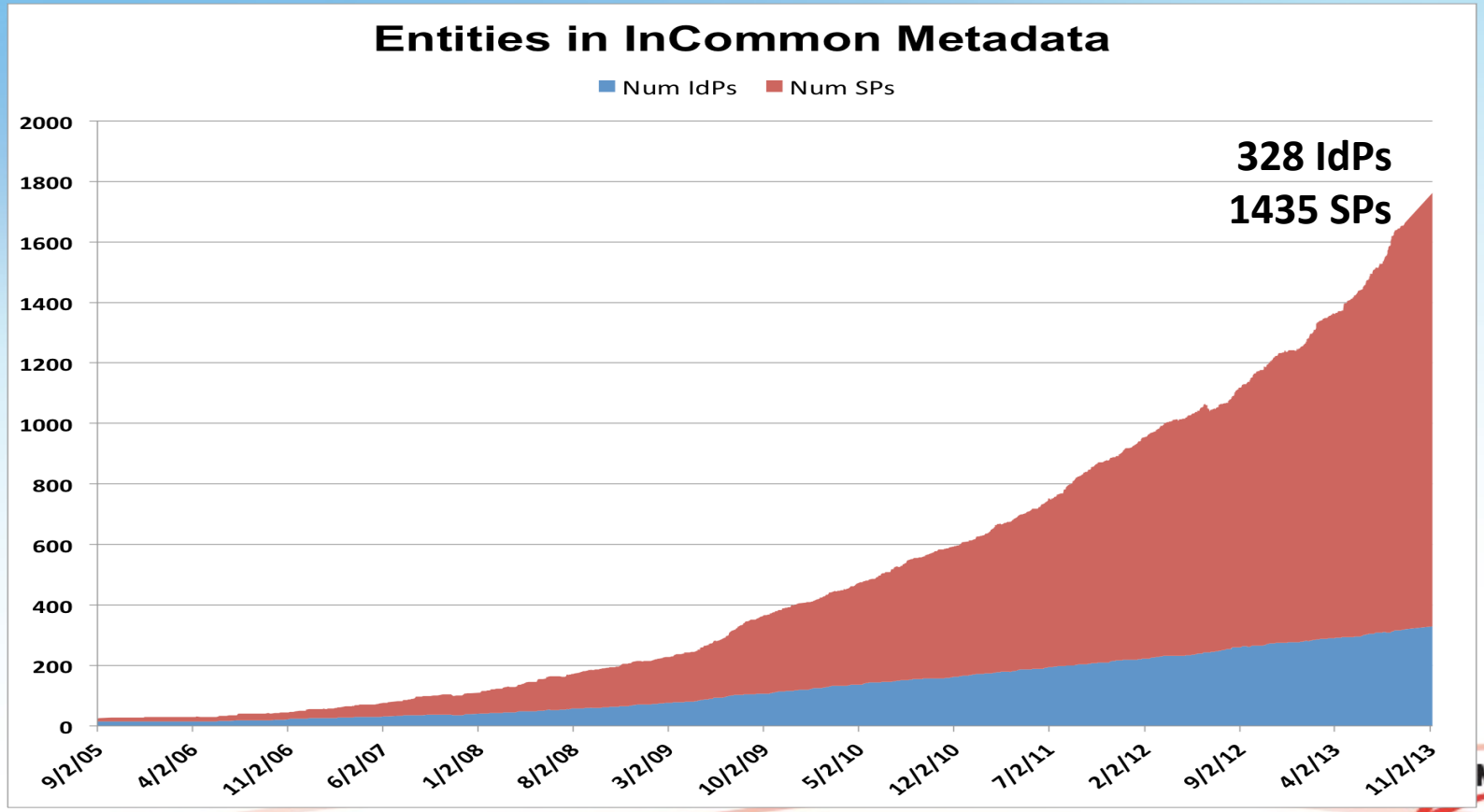
CN	CARSI
IN	INFED
LT	LEFT
MA	eduIDM
PL	PIONIERId
RO	RoEduNet Federation

InCommon today

InCommon®

- 400+ universities, 600 + total participants, growth continues strong
  - Many cloud service providers, from Microsoft to Elsevier to NIH and NSF to ***
- > 6-7 M users
- Primary uses:
  - Outsourced services, government applications, access to software, access to licensed content, etc.
  - Access to wikis, shared services, cloud services, calendaring, command line apps, medical, etc.
  - A basic requirement for cloud services
- FICAM certified at LOA 1 and 2 (Bronze and Silver).
- New services
  - Certification marks - R&S (Research and Scholarship)
  - Multi-factor authentication support (devices, software, etc)
  - Certificates – SSL and Personal
  - InCert - open-source client-cert lifecycle management

INTERNET 2


Entities in InCommon Metadata
Num IdPs
Num SPs
328 IdPs
1435 SPs
2000
1800
1600
1400
1200
1000
800
600
400
200
0
9/2/05
4/2/06
11/2/06
6/2/07
1/2/08
8/2/08
3/2/09
10/2/09
5/2/10
12/2/10
7/2/11
2/2/12
9/2/12
4/2/13
11/2/13

US Government Efforts

- FICAM
  - Classic identity services for government; slowly growing
  - Includes high assurance PIV cards and PKI, federated identity, the F6 Gateway, etc.
  - Provides the LOA certifications that motivate the InCommon assurance program, including Silver
- NSTIC
  - Aimed at Next Gen – services, privacy, etc.
  - Has distinct governance and pilots efforts
  - Scoping is a finesse: affecting government identity

INTERNET 2

NSTIC Pilots – Round 1

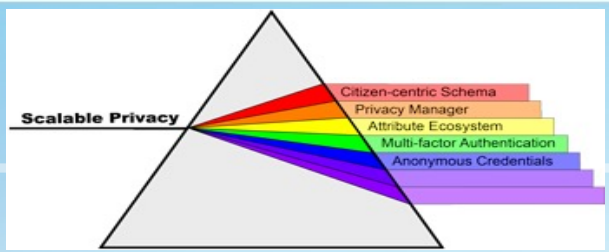
- A variety of efforts, some highly experimental business models, some foundational infrastructure. Most are private partnerships, with limited visibility into their efforts
- Third-party ID verification that uses drivers' licenses and state motor vehicle departments for authentication.
- *Commercial, open-source ID verification network that allows multiple relying parties to verify a user's identity by referring to the authoritative sources.
- Multi-factor mobile authentication that uses varying levels of trust from PINs to geolocation.
- Data encryption with broker verification that enables access to personally identifiable information.
- **Scalable privacy - https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy+Home

NSTIC Pilots – Round 2

- GTRI
  - Trust frameworks
- PRIVO
  - A minor's trust framework
- Troop.id
  - Identity for Armed Forces
- TSCP
  - Transglobal Secure Collaboration Participation
  - Trustframeworks
- Exponent
  - Devices as identity (phones, rings, bracelets, teeth)

INTERNET 2

Scalable Privacy



- 2+ year grant to Internet2/InCommon
- Development partners are CMU, Brown, with expertise from Wisconsin, Ohio State and others
- Several focal points
  - Promotion of multi-factor authentication
  - Citizen-centric attributes and schema
  - Development and deployment of privacy managers
  - Introduction of anonymous credentials
- https://spaces.internet2.edu/display/scalepriv

Work described in this presentation is supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST). The views in this presentation do not necessarily reflect the official policies of the NIST or NSTIC, nor does mention by trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

INTERNET

Scalable Privacy deliverables

- Promotion of two factor authentication
  - Good privacy begins with good security
- Citizen-centric attribute activities
  - For transactions, for accessibility, for social government
- Trusted metadata approaches
  - Conveying trustmarks about the relying party and the Identity Provider, vetted by the federation and by third-parties
  - Structured around trust elements
- Next-generation privacy manager
  - Leveraging prior work, trusted metadata, usability-built-in
- Anonymous credentials
  - Evaluate issues in integrated deployments at scale

INTERNET 2

Promotion of multi-factor authentication (MFA)

- Good privacy begins with good security
- MFA addresses a significant number of security threats
- A variety of second factor alternatives are now viable – USB devices, NFC devices, cell phones, certificates, etc., and technology can bridge across them
- Power of coupling MFA and Federated identity
  - Combining MFA with WebSSO and federated identity allows MFA to be leveraged by many services/SPs; “MFA externalities”
  - Potential to help achieve higher levels of assurance
  - If biometric factors are used, “privacy spillage” limited to IdP

INTERNET 2

MFA: Two major thrusts

- MFA Pilot Institutions: support wide-scale deployments of MFA technologies at three institutions:
  - Massachusetts Institute of Technology (MIT)
  - University of Texas System
  - University of Utah
- MFA Cohortium: Create and facilitate a cohort of additional institutions, establishing a collaborative environment for sharing questions, requirements, planning, expertise, experience, artifacts, etc. related to deploying and supporting MFA, leveraging the pilot institution activities.
  - Now ~ 40 institutions, > 1M potential users
  - Creating a next generation of MFA aware users
  - Technology agnostic, lifecycle oriented
  - https://spaces.internet2.edu/display/mfacohortium

INTERNET 2

Early interesting issues in MFA at scale

- Accessibility support
  - From device issues to accessing preferences during MFA processes
- FERPA issues in the release of PII (e.g. cell phone number) to third party authenticator
  - More generally the legal relationship between enterprise and third party authenticators
- Cloud authenticators and DDOS attacks
  - Should enterprise authn fail under external DDOS?
  - Generally, identifying key barriers to outsourcing components of authn
- Alternative strategies when multifactor tokens aren't available
  - MFA fails more frequently, if only for environmental issues
  - "Fallback" approaches for opt-in deployment models?
- ROI of federated MFA
  - The leverage of federation and MFA is enormous, but how to capture it?

INTERNET 2

Three important software deliverables

- Shibboleth-based integrated, universal MFA handler
  - Shib is the most widely used open source federating software platform in the world
  - Multilateral Shib-based federations exist in over 40 countries, in real estate, in government, in law enforcement, in securities and banking, etc
  - A universal well-integrated MFA handler instantly opens MFA externalities
- CAS integrated, universal MFA handler
  - CAS is a very widely used open source SSO
- InCert
  - Open source client certificate lifecycle management system
  - Also provides device boarding and device security
  - Client certs are invaluable for many ecosystem capabilities beyond authentication and anti-phishing
  - http://www.internet2.edu/incert/
  - https://spaces.internet2.edu/x/vAhOAg

Citizen-centric attribute deliverables

- Schema Catalog and Attribute Registry
  https://spaces.internet2.edu/x/dgROAg
  http://macedir.org/ontologies/attribute/2012-11-10/attributeOntologyDoc/
- Attribute-annotated Use Cases
- Cookbook "To Serve Citizens" ☺
- Global Public Inclusive Infrastructure (GPII) Proof of concept, using User-Managed Access (UMA)
- Bindings and refactoring
- Engagement with the privacy manager

INTERNET 2

GPII Proof of Concept

- The purpose of the Global Public Inclusive Infrastructure (GPII) is to ensure that everyone who faces accessibility barriers due to ***disability***, ***literacy***, ***digital literacy,*** or ***aging***, regardless of ***economic resources***, can access and use the Internet and all its information, communities, and services for education, employment, daily living, civic participation, health, and safety
- Automatic personalization of user interfaces and user context adaptation based on user preferences, across platforms
- Schema standard is AccessForAll (ISO/IEC JTC1 24751)
- http://gpii.net
- Pilot applications, proofs of concept beginning with
  - User preferences stored and accessed securely in an online repository
  - Those preferences drive presentation features that provide accessibility accommodations when user visits online resources
  - All leveraging UMA profiles of Oauth 2.0 aligned with emerging GPII security and privacy architectures

INTERNET 2

What we hope to learn in the next year

- Annotate additional use cases
- Foster some convergence discussions
- Develop key data-driven issues:
  - In R&E, IdP's are normalized (syntax and semantics) on key attributes but are attribute retentive in what we release to others; in the social space, IdP's are wildly divergent on attributes but generally promiscuous in which attributes are released.
  - Is there a hierarchical "sweet spot" where users can actively manage privacy with almost no impedance?
  - Internationalization issues, from policy to the Spanish surname topic
- Foster active research on usability within the academic community
- The relationship of citizen-centric attributes to provisioning data

Privacy managers (Carnegie-Mellon University)

- Consoles to help users manage the release of attributes
- Can leverage trust, informed consent, default settings and preferences, etc.
- Must be carefully engineered
  - Across the variety of contexts
  - Across a variety of credential types
  - In ways that are user-effective
- Similar, less leveraged approaches are successfully deployed in a few settings, demonstrating that users can and will manage privacy.
- Research shows that over 90% of social network users do not know what attributes are being released or how to change it

INTERNET 2

Key design considerations

- Usability
- CMU Tech Report, Warning Design Guidelines, Bauer et al
- Informed and * consent
- GPII
- Technology agnostic – SAML, anon creds, OpenId, etc., though plumbed to Shib to start
- Awareness of out-of-band considerations
- “Nudging” applied to privacy
- Minimal disclosure for constrained purpose
- First alpha due this month

INTERNET 2

Carnegie Mellon University

CMU's Calendar is asking CMU for your

Andrew ID* (**lujo**)	will send
~~credentials to access CMU services~~	won't send
~~full name (**Lujo Bauer**)~~	won't send
and CMU affiliation (**faculty**)	will send

Use the toggle switches to select the items that will be sent to CMU's Calendar. Items marked with * are required to access and personalize the calendar and cannot be unselected.

Continue to CMU's Calendar?

Yes No Explain

INTERNET 2

Carnegie Mellon University

CMU's Calendar is asking CMU for your

Andrew ID* (**lujo**) will send

credentials to access CMU services will send

full name (**Lujo Bauer**) will send

and CMU affiliation (**faculty**) will send

Use the toggle switches to select the items that will be sent to
with * are required to access and personalize the calendar anc

Continue to CMU's Calendar?

Yes No Explain

Information

CMU's Calendar needs your Andrew ID in order to provide the desired service. CMU's Calendar cannot function properly if an Andrew ID is not supplied.

CMU's Calendar will not use your Andrew ID for any other purpose, and will not keep this information after you close the window.

Your Andrew ID is "[lujo]". If you continue to CMU's Calendar, your Andrew ID will be sent to it.

Click here to contact an administrator if you have further questions or believe this information is incorrect.

INTERNET 2

Metadata and trust implications

- At scale, there needs to be ways to establish and convey trusted information about applications and services to users
  - Implies "vetting" or auditing processes for services
  - Implies metadata that can convey this information in real time to users
  - Implies trust in the metadata
- Dynamic metadata services
  - Work is already underway on this in other places
- Federation operations need to evolve
- Auditing applications
  - For "privacy-preserving" approaches (minimal attribute requests, informed consent, proper handling and disposal, etc.), for COPPA compliance, for …
  - Two marks now: Research and Scholarship, Service by Affiliation

INTERNET 2

Next Steps

- Starting a major engagement with a set of cutting-edge campuses on opportunities and issues for deployment at scale.
- “Lifestyles of the Attribute Rich and Privacy Preserved” (LARPP)
- Will address opportunities and issues across the full range of “products” in both institutional and federated use cases
- Intended to develop advanced approaches in areas including
  - Deploying active end-user privacy management
  - Scalable inter-institutional access control through attributes
  - Use of anonymous credentials for institutional attestations, local medical records, etc.
  - New accessibility approaches
  - International privacy laws reconciliation
  - Others as they arise

INTERNET 2

Of trust frameworks, marks and elements

- Trust frameworks and trust marks are ambiguous and misconstrued terms.
- What we have some understanding of is many of the trust elements that can be used, in concert, to build frameworks and marks.
- The elements fit well into a periodic table showing the issues (e.g. legal, privacy, operational) that they address
- There are new elements still be discovered, and the organization of the table is malleable
  - E.g. Hub and spoke versus multi-lateral federations
- Trust marks combine elements necessary to address a thematic issue, such as accessibility, COPPA compliance, etc.
- Marks are likely static, though news ones will occur
- Frameworks are more dynamic, as the COI evolves its business and needs to address new trust elements.

INTERNET 2

Aspects of the Periodic Table

- Most current version of the periodic table is athttps://spaces.internet2.edu/display/scalepriv/
- Rows represent scale, from the relatively few federated operators at the top to the thousands of organizations and millions of users at the bottom
- Colors represents business functional areas, including technical, operational, policy, legal, etc.
- Clusters of elements represent related sets of issues, such as the technical requirements needed to trust attribute authorities within a federation
- No underlying metric such as atomic weight.

INTERNET 2

Interfederation

- The steady state of federated identity is “interfederated identity”
- Interfederation across countries in the same vertical.
- Interfederation between sectors (R&E and K-12; R&E and healthcare; R&E and government).
- Key technology change is the move from static metadata bundles (ala /etc/hosts) to dynamic metadata (ala DNS)
  - Standards and code are now moving forward
  - Exchange points are being shaped
- Key policy issues are in the periodic table –
  - E.g. Europe is advancing adjudication in the identity provider country; every SP in the US could be challenged.
  - Privacy issues are particularly hard

Social2SAML

- Social2SAML gateways
  - Converts social identities (e.g. Google, Yahoo, MSN, Facebook) into SAML assertions
- Very handy for extended populations
- Exposes many issues with social identity that require careful thought.
  - Coarse grain release versus fine grain release
  - Promiscuous attribute release; inconsistent attribute release
  - Conversion of identifier types
    - Implications of persistency, etc
    - What's in a name
  - LOA mapping

INTERNET 2

Scholarly identity

- Application categories
  - Research and Scholarship
  - Service by Affiliation
  - eduPerson (201310) has been formally released
- CILogin
  - Converts federated identity into grid credentials for national compute and data stors
  - www.cilogon.org
- eduPerson and ORCID
  - Discussions now underway about including it in the eduperson schema as an attributes
  - Issues about self-asserted vs institutional, multi-value, etc being explored

ORCID in the attribute ecosystem

- Orcid.org vision is two-fold
  - ORCID identifier as a bridge identifier to create persistent associations between a researcher and the researcher's accumulating body of work
  - ORCID.org envisioned as the authoritative source of crosswalks between researcher identifiers from multiple sources
    - ORCID, Thompson Reuters, Scopus, Harvard Profiles,…
    - Through one-on-one cross-organizational outreach and collaborative projects
- Two main paths by which researchers obtain ORCID identifiers
  - Self-registration at the ORCID site
  - Institutionally assigned (e.g. to entering grad students, new faculty hires)
  - Once assigned, the ORCID identifier belongs to the person, not the institution
  - Multiple ORCID ids per researcher will be a reality; that will create the need for a ORCID identifier linking service (hosted by ?, Self-service?)

INTERNET 2

ORCID in the attribute ecosystem

- There are federated applications that would like to receive ORCID identifiers from institutional Identity Providers (IdPs)
  - ScienCV at NLM
  - What is the responsibility/risk taken on by an IdP that asserts ”scholar A’s ORCID id is xyz”?
  - If the ORCID identifier belongs to the researcher, the institution will have to provide a way for researchers to claim their ORCID identifier if they already have one
- MACE-Dir has begun the conversation around these issues
  - Choice between minting an attribute specifically for ORCID identifiers or defining a generic “Researcher Identifier” attribute to carry more than one type
  - Trade-offs between ease of processing by the relying party and burden on the IdP to craft and populate a variety of special purpose researcher identifier attributes (“Just look for the orcidId attribute or the scopusId attribute,…”)
  - If multiple types carried in a single “ResearcherIdentifier” attribute, thorny problem of indicating which type for which value. Has been challenging to find a widely supportable solution to this class of problem in LDAP entries and SAML assertions

INTERNET 2

ORCID in the attribute ecosystem

- If InCommon IdPs become able to assert ORCID identifiers, to which relying parties (RPs) should they release them?
  - An attribute release decision for the individual researcher?
  - ORCID identifier as one of the elements of a “Research and Scholarship” bundle of attributes to be released to RPs that are qualified as being in the “Research and Scholarship” category?

INTERNET 2

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.
- There are more groups than there are identities

INTERNET 2

Collaboration platforms

- Drive identity and access control for both general collaboration and domain-specific research apps
- Leverage existing IdM technologies
- Leverage existing IdM deployed infrastructure
- Offer a variety of implementation and deployment options
- Collaboration platforms can be run at national levels (e.g. UK, Australia, Netherlands), campus or local levels.
- https://spaces.internet2.edu/display/COmanage/Video

INTERNET 2

CoManage and CoCoA

- CoManage
  - An identity management system for virtual organizations and collaborations
  - Addresses identity and access control; leverages Shibboleth, federation, Grouper and …
- CoCoA (**Co**manage + **Co**next + **A**pplications)
  - Integrates Comanage with
    - Connext, an open source Dutch collaboration platform
    - Any domesticated application, including lists, wikis, audioconferencing, videoconferenceing, Google Docs, Al Fresco, Adobe Connect, doodle, command line, etc.

INTERNET 2

CoCoA

INTERNET 2

Takeaways

- Moving the needle on MFA
  - MFA and federation together a powerful combination
- Attributes are the key (and its already a mess)
- Researching what it takes to put the “informed” into consent, and trying to deploy it
- Anonymous credentials are still immature, and still the only answer to unobservability
- Social identity has its virtues and its perils
- Collaboration platforms are the access management part of IAM
- The eventual steady state future is “interfederated identity” but getting there will be fitful and indirect.