



June 5, 2013

Ken Klingenstein

Identity Management, the Cloud, NSTIC and Accessibility

Identity Management, the Cloud, NSTIC and Accessibility

Contents

- Internet Identity Today
- Two types of cloud use cases
- NSTIC and the Identity Ecosystem
 - Governance
 - Pilots
- Scalable Privacy
 - GP11
- The Attribute Ecosystem

Internet Identity Today

- Social identity, at least in the US, is reaching saturation, close to 100%
 - Emphasis is shifting to mining data for cross purposes, third party auth
 - Protocol may be evolving from OpenId to OpenId Connect
 - OAuth 2.0 to handle all the non-web and mobile apps
 - Continued efforts to climb LOA stack with MFA
- Federated identity with SAML continues to grow and dominate inter-organizational interactions
 - Other verticals building multi-lateral federations now
 - Interfederation is moving forward, slowly but steadily...
- Hybrids grow
 - Social2SAML and SAML2Social Gateways
 - New aggregators, e.g. PingOne, REEP

R&E federations lead the way

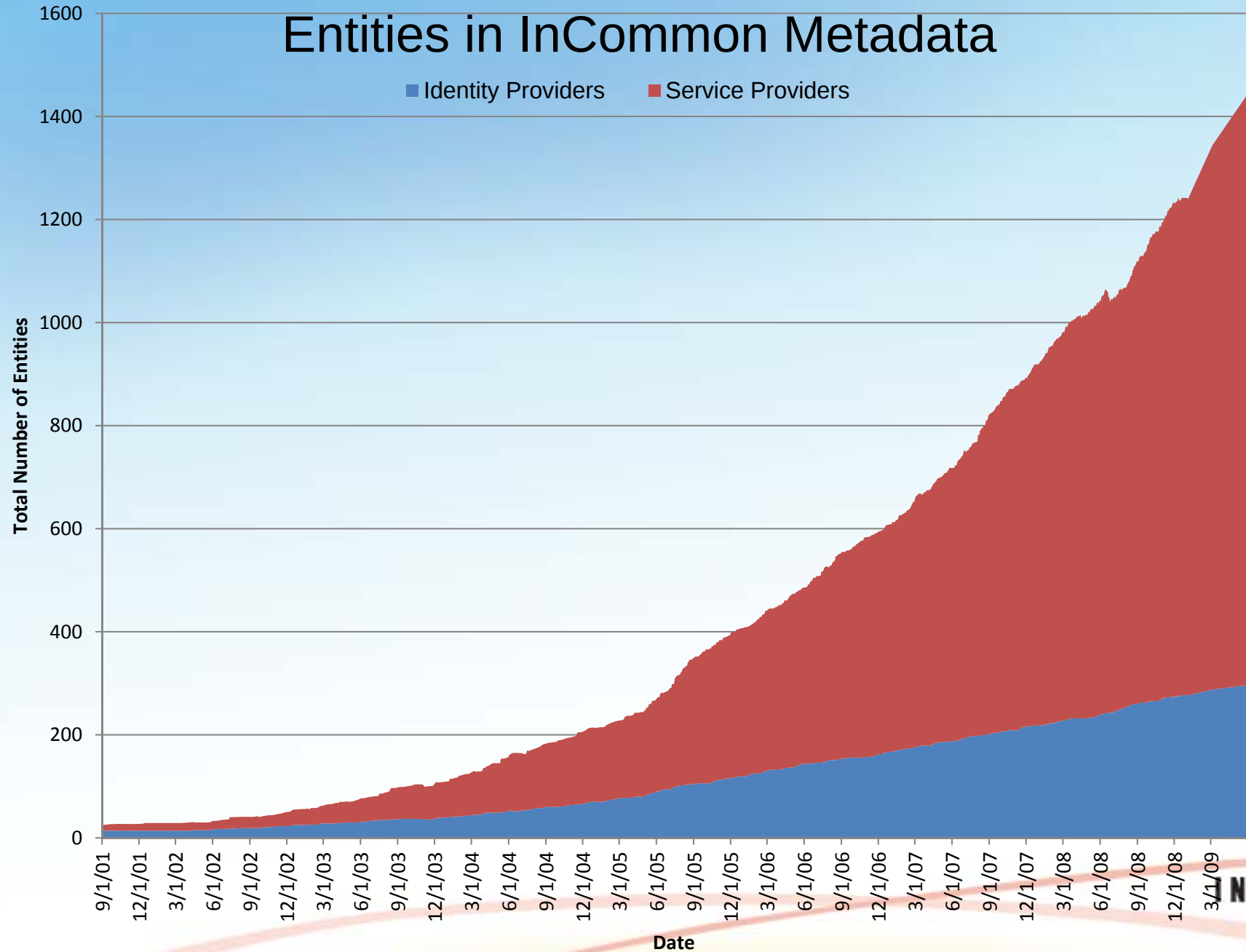
- Creating the protocols
 - Privacy preserving and attribute centered by design
- Thinking multilateral from the start
 - Its all about the metadata
- Managing Privacy
 - Attribute release managers
 - Certification of applications
- Integrating anonymous credentials
 - Way cool, way old technology may finally get deployed

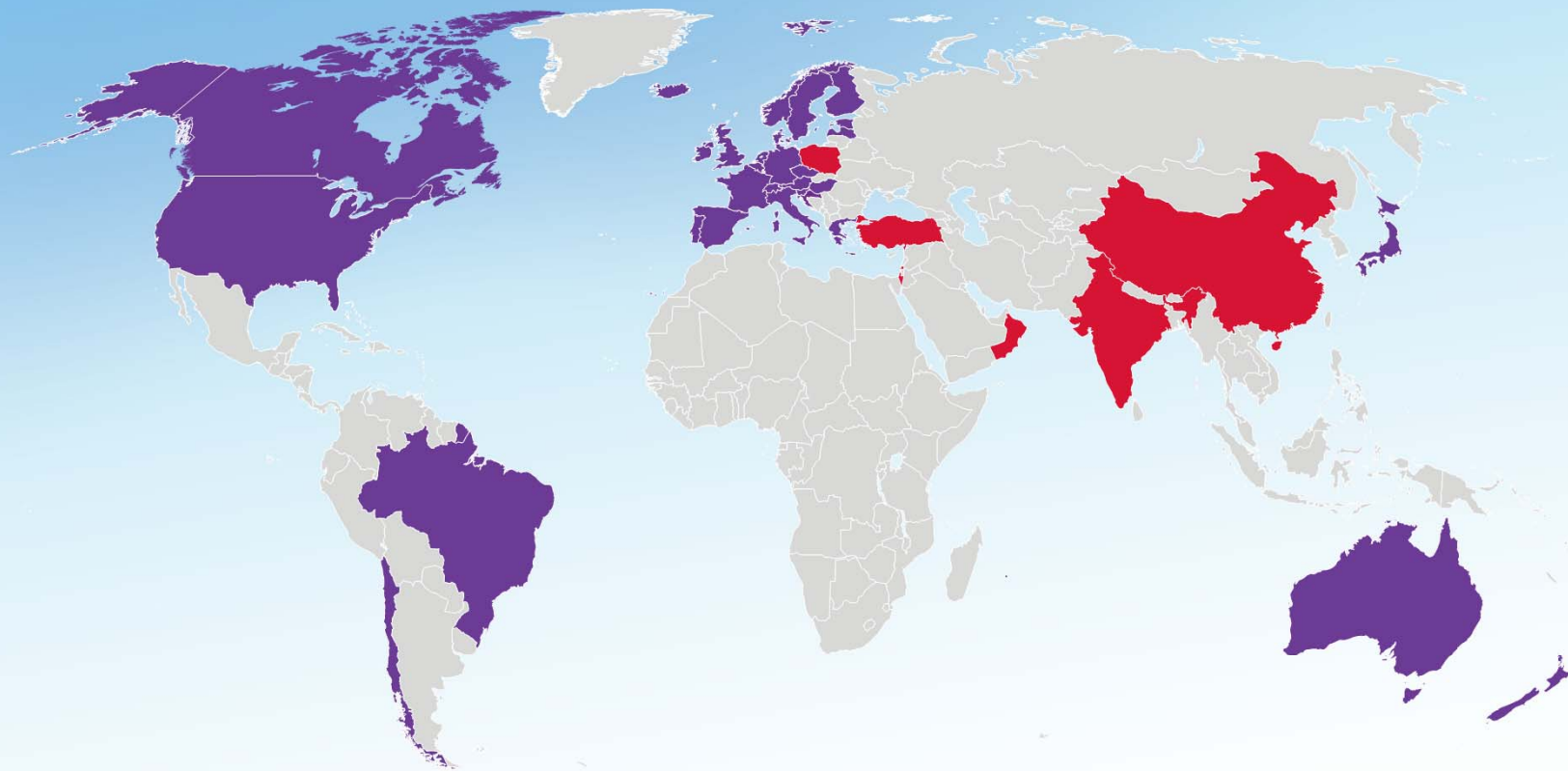
InCommon today



- 500+universities, 650+total participants, growth continues rapid
 - Many cloud service providers, from Microsoft to Elsevier to NIH and NSF to ***
- > 10 M users
- Traditional uses continue to grow:
 - Outsourced services, government applications, access to software, access to licensed content, etc.
- New uses bloom:
 - 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
 - Certificates – SSL and Personal
 - InCert - open-source client-cert lifecycle management
 - Certification marks - R&S (Research and Scholarship)

Entities in InCommon Metadata





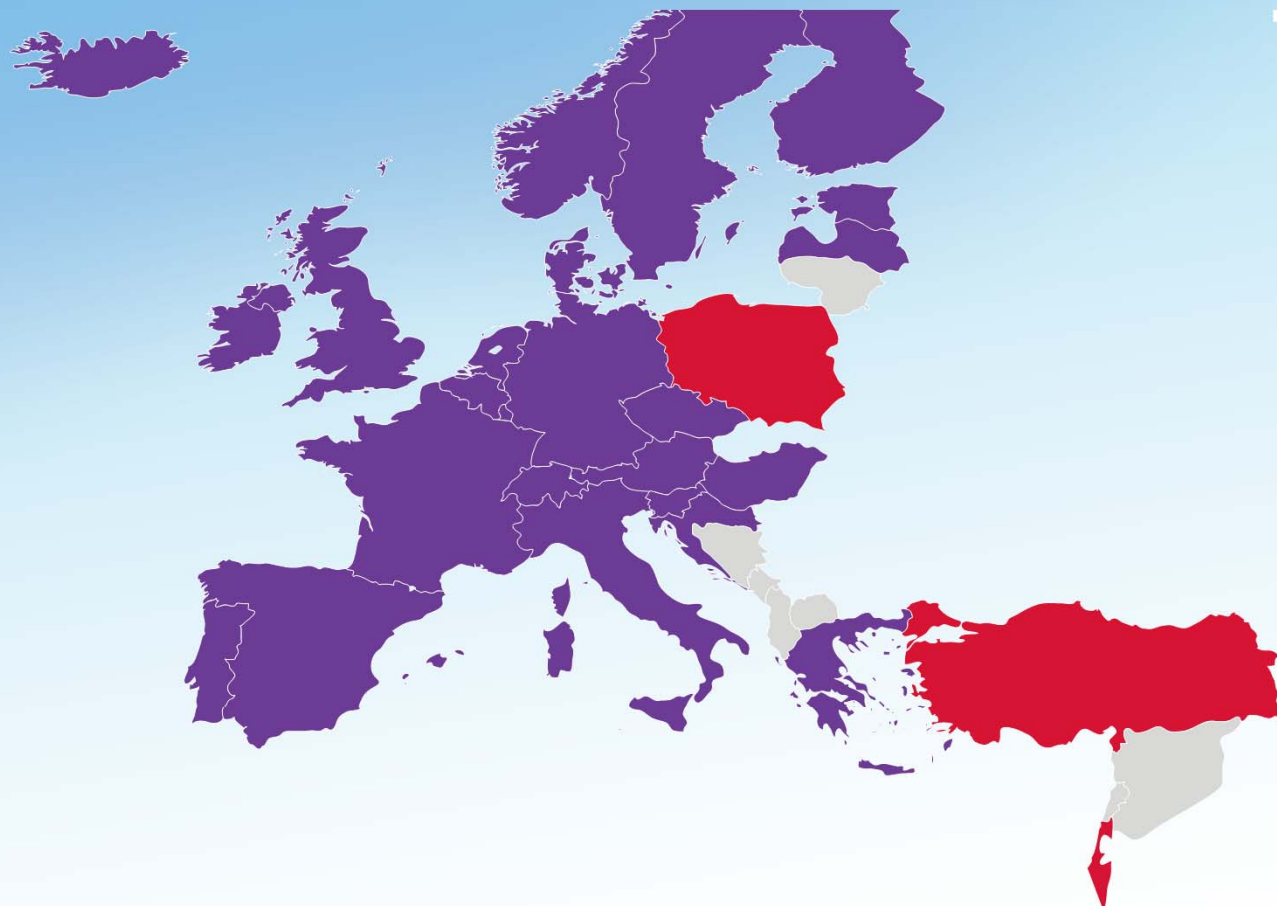
Identity Federations in production

AT	ACOnet Identity Federation	ES	SIR
AU	Australian Access Federation AAF	FI	Haka
BE	Belnet R&E Federation	FR	Fédération Éducation-Recherche
BR	CAFe	GR	GRNET
CA	Canadian Access Federation CAF	HR	AAI@EduHr
CH	SWITCHaai	HU	eduID.hu
CL	COFRe	IE	EduGate
CZ	eduID.cz	IT	IDEM

NL	SURFfederatie
NO	FEIDE
NZ	Tuakiri New Zealand Access Federation
PT	RCTSaai
SE	SWAMID
SI	ArnesAAI Slovenska
UK	UK Access Management Federation for Education and Research

Identity Federations in pilot

CN	CARSI
IN	INFED
OM	Oman Knowledge ID Federation
PL	Poland Identity Federation
TR	ULAKAAI
IL	IsraGrid Federation



Identity Federations in production

AT	ACOnet Identity Federation	FI	Haka	NL	SURFfederatie
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

PL	Poland Identity Federation
TR	ULAKAAI
IL	IsraGrid Federation

Internet identity takeaways

- Be protocol agnostic
 - SAML for business, OpenId* for consumer, and gateways galore
- What matters are payloads and metadata
 - Payloads are attribute values, rich in capabilities
 - Metadata for everything to scale
 - Federation, access control, privacy management, accessibility, etc
- Multilateral federation and interfederation will be steady state
 - R&E multilateral from the outset, and DoJ++ an early adopter
 - Other verticals now moving from bilateral to multilateral, including securities, real estate, pharma
 - Interfederation across verticals and internationally
- Monetization is big, at least in the US
 - Number of IdP's (4 to 1M)
 - Selling of information and preferences
 - Europe has a different culture, and confused legislation

Two distinct “cloud” use cases

- User to cloud service – SAAS
 - Services and content
 - Salesforce, Amazon, Ebay, Hathitrust, MS, etc.
 - Issues are bi-lateral
- User to user via the cloud
 - Collaborations and interaction
 - Facebook, Twitter, Google+ are closed examples
 - Wikis, massive collaboration platforms are open examples
 - Issues are multi-lateral
- What issues?
 - Metadata, trust, privacy, accessible at birth, etc.

US Government Efforts

- FICAM
 - Classic identity services for government
 - Steadily growing, successful
 - Includes high assurance PIV cards and PKI, federated identity, 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
 - Applicable more broadly than just US Gov services

NSTIC

- National Strategy for Trusted Identities in Cyberspace – major White House Initiative on citizen-gov security/privacy
- Scoping is a finesse: affecting government identity interactions (along with FICAM), influencing a commercial marketplace, influencing a global identity ecosystem
- Has both governance and development components
- OMB Directive issued Fall of 2011 to move to external identities where appropriate
- www.nist.gov/nstic
- Faces challenges with limited resources, ambiguities in scope, the Facebook ToS, existing business models, etc.
- The vision works for R&E needs...
 - A placemat from an Ethiopian restaurant in DC in 2001

NSTIC Governance

- Intended to define the rules for electronic identity transactions, at least with the federal government, but more broadly as anchor tenant for the general marketplace
 - Privacy, security, robustness, usability, standards, etc.
- Most of the big players, across identity providers, relying parties, state and local governments, businesses from start-ups to Mastercard and Microsoft to ACLU, EFF, CDT, etc.
- Had to navigate public-private partnership, NPO status, IPR, elections, etc.
- Wrapped around axles of role, authority, processes for a long time; now moving a bit into substance.
- www.idecosystem.org

NSTIC Pilots

- Grants to develop aspects of the Identity Ecosystem – from privacy to monetization, from government to business, from hardware approaches to citizen use...
- Five grants awarded in September 2012
 - <http://gcn.com/Articles/2012/12/19/5-elements-identity-ecosystem.aspx?Page=1>
- Very different world views represented
- Scalable Privacy award to Internet2/InCommon
 - <http://gcn.com/Articles/2012/12/19/5-elements-identity-ecosystem.aspx?Page=5>

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>

Scalable Privacy

- Two 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
 - Introduction of anonymous credentials
 - Development and deployment of privacy managers
 - Citizen-centric attributes and schema
- <https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy+Home>

Citizen-centric attribute deliverables

- Schema Catalog and Attribute Registry
- Attribute annotated Use-Cases
- Cookbook “To Serve Citizens” 😊
- GPII Proof of concept
- Bindings and refactoring
- Engagement with the privacy manager

Categories of use cases

- Accessibility
 - Physical, cognitive, age-related, etc.
 - Global Publically Inclusive Internet (gpII.net)
- Operational Government
 - Transaction based
 - May be out of scope
- “Social Government”
 - Community wikis, on-line discussions, news feeds, etc
 - Generally local in nature, often requiring anonymous but attribute-controlled access (e.g. resident, registered voter, over legal age, etc.)
- Envision It Scenarios
 - Contained in Full NSTIC Strategy (April 2011)
 - http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
- UMA developed
- IdeSG provided – see

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 (ISO/IEC JTC1 24751)
- gpii.net
- Proof of concept will establish user preferences stored in an authorization server being used with open credentials to adaptively present content

Privacy managers (Carnegie-Mellon Univ)

- 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.

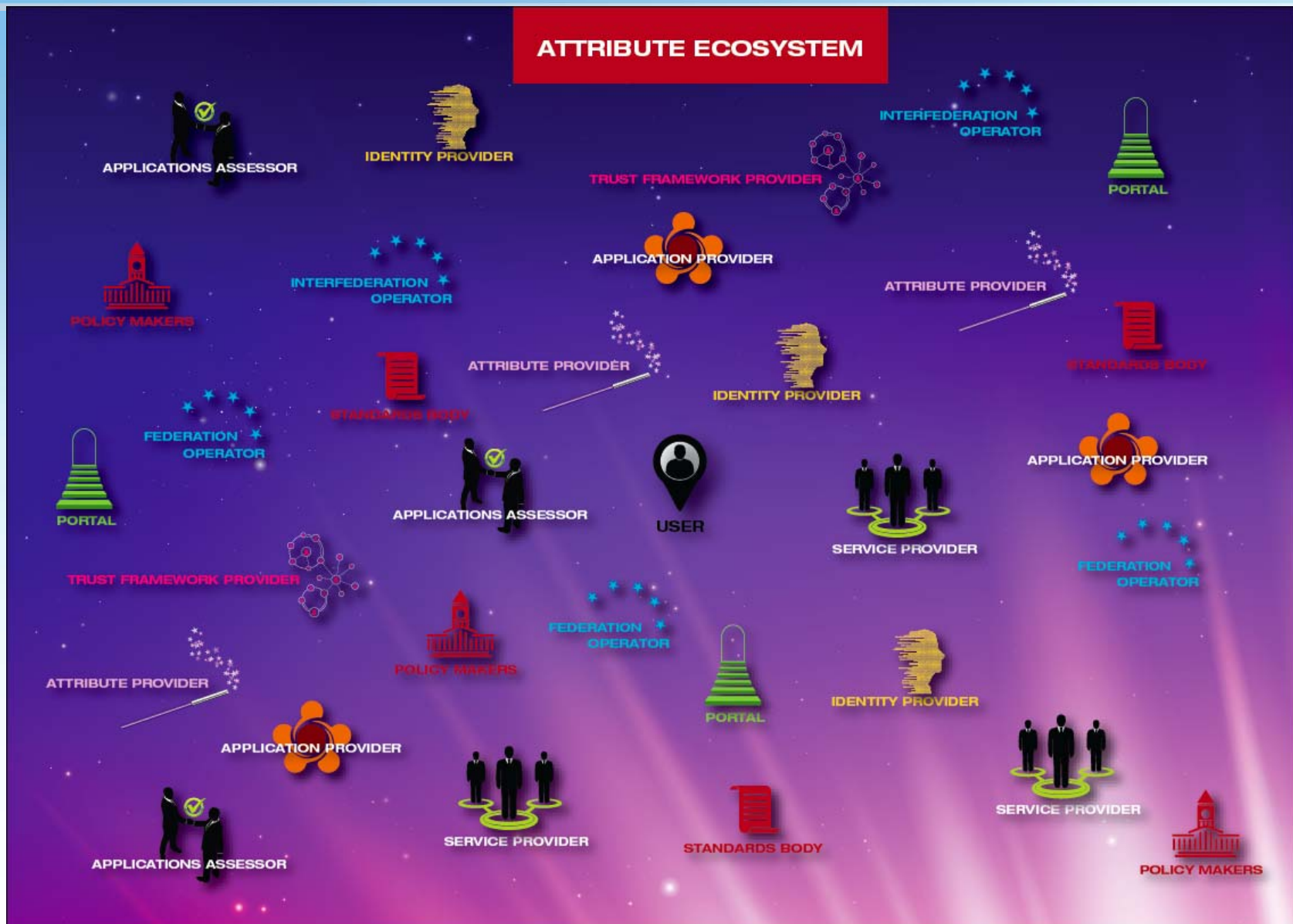
Key design considerations

- Usability
- [CMU Tech Report, Warning Design Guidelines, Bauer et al](#)
- Informed consent
- GPII
- MFA
- Awareness of out-of-band considerations
- “Nudging” applied to privacy
- Minimal disclosure for constrained purpose

The Attribute Ecosystem

- Those parts of the identity ecosystem that focus on attributes in the ecosystem
- Centers on the creation, exchange and use of attributes associated with those in the identity ecosystem
- Critical to privacy, scalable access control, accessibility, etc.
- Depends heavily on other aspects of the identity ecosystem, including authentication, trust, etc.
- The relatively unexplored part of the landscape.
- The framing for Accessibility and the Cloud architectures

A part of the attribute ecosystem



Elements of the Attribute Ecosystem

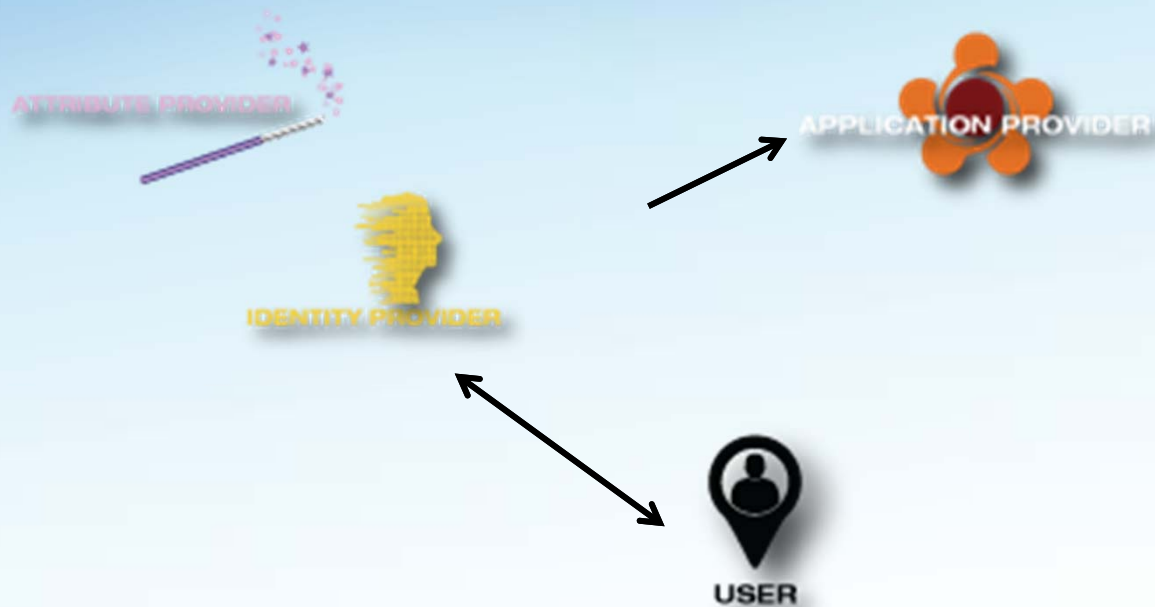
(an evolving understanding)

- IdP' s
- SP' s
- Attribute authorities and providers
- Attribute verifiers
- Trust frameworks and trust framework providers
- Third parties, portals, etc.
- Federation operators
- Application auditors
- The user, and, if applicable, the subject

What Flows Within the Ecosystem

- Attributes
 - May be externally asserted (e.g. student, citizenship), self-asserted (e.g. preferred language), third party asserted (e.g. resident of a town), accessibility, etc.
- Management of attributes
 - Trust, certification marks and vetted application information, user consent flows, etc.
 - Can flow as metadata or in-stream

Standard enterprise attribute flow



Associated metadata and trust flow

