Identity Management: Background, Principles, GENI

INTERNET®

Topics

- Internet identity
  - What's been happening
  - Gaps
- Identity Management
  - Includes identity and access control via groups and roles
  - Adapting apps to use external attributes - domestication
- Some Identity Management Principles
- Some GENI Identity Management Principles

kjk@internet2.edu

In the last few years…

- Internet identity has become pervasive, in two flavors
  - A rapidly growing, but still maturing federated identity infrastructure, particularly in the R&E sector globally.
  - A set of theoretically interoperable social identity providers serving large masses of social and low-risk applications
- Uses vary by country and sector
  - In some countries, 100% of citizens, using for government, research, educational and other uses
  - In the US, extensive internal government use expanding to R&E
  - Verticals building federated corporate identities

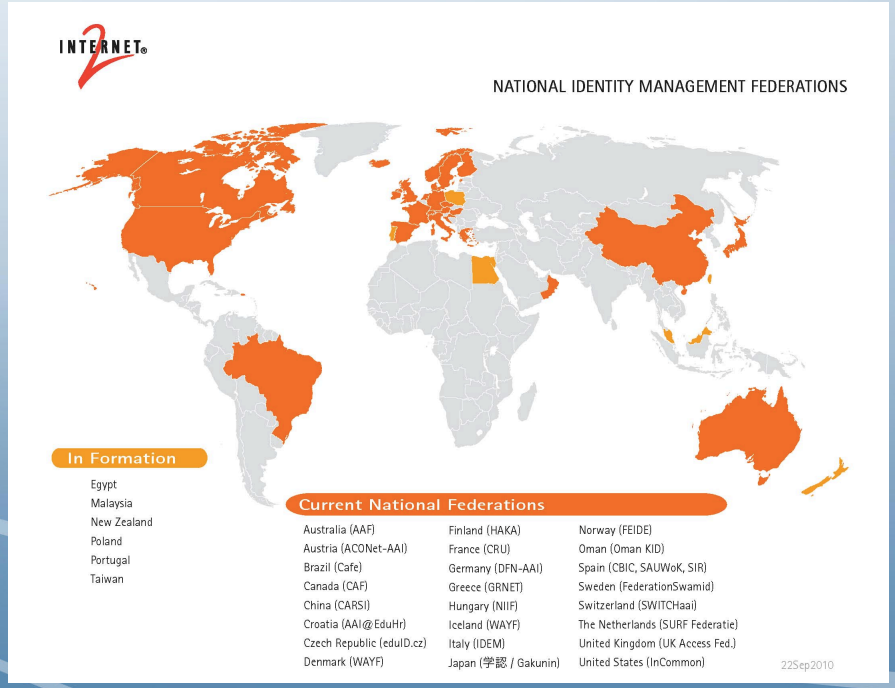
kjk@internet2.edu

Internet scale

- 6 M users, 250 organizations in InCommon
- R&E Federations in Europe and Asia are more extensive, spanning 25 countries and tens of millions of users.
- Social identities, including Facebook, Google, Twitter, Yahoo, Paypal, etc are legion
- Anchoring government applications now emerging
- Standards processes in IETF, OASIS, Kantara, etc.
- Powerful drivers, valid business models indicate long-term global infrastructure emerging

kjk@internet2.edu

SAML federations worldwide - scope



kjk@internet2.edu

Where We Headed

- The trust infrastructure
  - An international peering of SAML R&E federations, with common attributes and LOA, with some careful integration of other identity approaches (e.g. OpenId).
  - Privacy preserving real time interrealm authentication and attribute exchange across all applications
- The collaboration/VO IdM overlay
  - Services that provide integrated VO identity and access management to both domain and collaboration apps
  - Leverages trust infrastructure, enterprise and VO attributes,etc

kjk@internet2.edu

Access Control at Scale

- Group management tools covers 80% of the use cases; privilege management covers most of the rest
- Two part process for an Internet-scale approach
  - Domestication of applications
  - Ways to construct and flow attributes across the Internet
- Can capture a variety of key concepts: fine-grain delegation, prerequisites, entitlements, quotas and throttles, life-cycle maintenance, etc.

kjk@internet2.edu

It is a work in progress

- Still immature
  - Not all institutions are in a federation
  - Not all institutions populate all base-level attributes
  - User-managed attribute release beginning
- Still gaps
  - Non-web apps just getting standardized by IETF (GSSAPI enhancements, enabling federated SSH)
  - Interfederation
  - Social2SAML

kjk@internet2.edu

Some Identity Management principles

- Need to scale
  - Users, applications, complexity
  - Truly Internet-scale infrastructure
- Need to address emerging privacy issues
  - Consent is a frequent requirement
  - International issues are real and confused
- Leverage institutional attributes
  - For accuracy as sources of authority
  - For accountability and audit
- Provide identity (LOA) consistent with security requirements

INTERNET®

kjk@internet2.edu

GENI IdM principles

- A need to create GENI specific and cluster specific attributes
  - Attributes need life-cycle maintenance processes
- A need to integrate across a set of existing GENI projects
  - A lot of horses have left the barn
- The need to present GENI infrastructure to other communities of users
  - Make GENI resources available within VO's, to campuses, to other agencies
  - International community

kjk@internet2.edu

Some terms

- Federated identity
  - Authenticate at home institution at appropriate level
  - Controlled release of institutional attributes
- Attributes
  - Institutional
  - Collaboration based
  - Self-asserted

kjk@internet2.edu

Collaboration Management Platforms (CMP)

- An important complementary local piece
- A person registry with automated life-cycle maintenance
  - Includes provisioning and deprovisioning
- A place to create, maintain local attributes
  - Using Groups and Roles
- A place to combine local and institutional attributes for access to applications
- A place to push/pull attributes to domesticated applications
  - Domain apps – SSH, Clusters, Grids, iRods, etc.
  - Collaboration apps – wikis, lists, net meetings, calendars, etc
  - Access via SAML, LDAP, X.509, etc

kjk@internet2.edu