A Future for InCommon: Products and Services

INTERNET®

Future of InCommon Topics

- InCommon Products and Services (Ken)
  - Advocacy, outreach and leadership
  - Foundational development
  - Trust Services
- InCommon Process, Governance, Membership – (Jack)
  - Process and Report
  - Internet2 Board and management responses
  - Next steps and outstanding issues

kjk@internet2.edu

Three categories of future work

- Leadership, Advocacy, Outreach
- Foundational – Core IdM middleware development, integration with other open source efforts
- Trust Services - basic federation operations, Silver and Bronze, Certificate Services, Training and Consulting, etc.

kjk@internet2.edu

Leadership, Advocacy and Outreach

- Leadership for InCommon and for Foundational Activities
- Work with federal partners
- Work with higher ed and research partners
- Work with corporate partners
- Work with international partners
- CAMPs, workshops, conference sessions

kjk@internet2.edu

InCommon as advocate

- Silver
- Need to have campuses provide persistent opaque identifiers (eptid)
- Need to adopt some explicit privacy approach, likely in the format of best practices and self certification
- Need to develop audit training mechanisms
- Active user privacy management

kjk@internet2.edu

InCommon and incident handling

- “Requirement” of Grid facilities
- Elements of an answer
  - Trust
  - Local enforcement of external requests
  - Interactions with law enforcement as needed
- How to amend InCommon agreements and processes

kjk@internet2.edu

Foundational Activities

- Maintain and evolve core software for IdM and federations
- Maintain and evolve core data standards for InCommon
- Work closely with overseas, open source and corporate developers

kjk@internet2.edu

Core software for IdM

- Systems that provide common identity services (identity, groups and privileges) for enterprise, domain and collaboration apps
- Shibboleth, Grouper, Privman (*), COmanage
- (Note – other important packages in this space include Kerberos, CAS, LDAP, etc.)

kjk@internet2.edu

The US role is shifting in IdM

- International development
  - Shibboleth – uApprove (Switch), SimpleSAML (Norway), Attribute aggregation (Switch), Delegated assertions Java library (Unicon), Inter-federation (GEANT), etc
  - Grouper – UI (UK), Sun IdM connector (Germany), web services validation (UK)
  - Components from Sweden, France, Dutch, etc…
- New use cases, new ways of interacting with partners
  - Integration with uPortal
  - Integration with KIM – Grouper and PACCman

kjk@internet2.edu

Shibboleth Futures

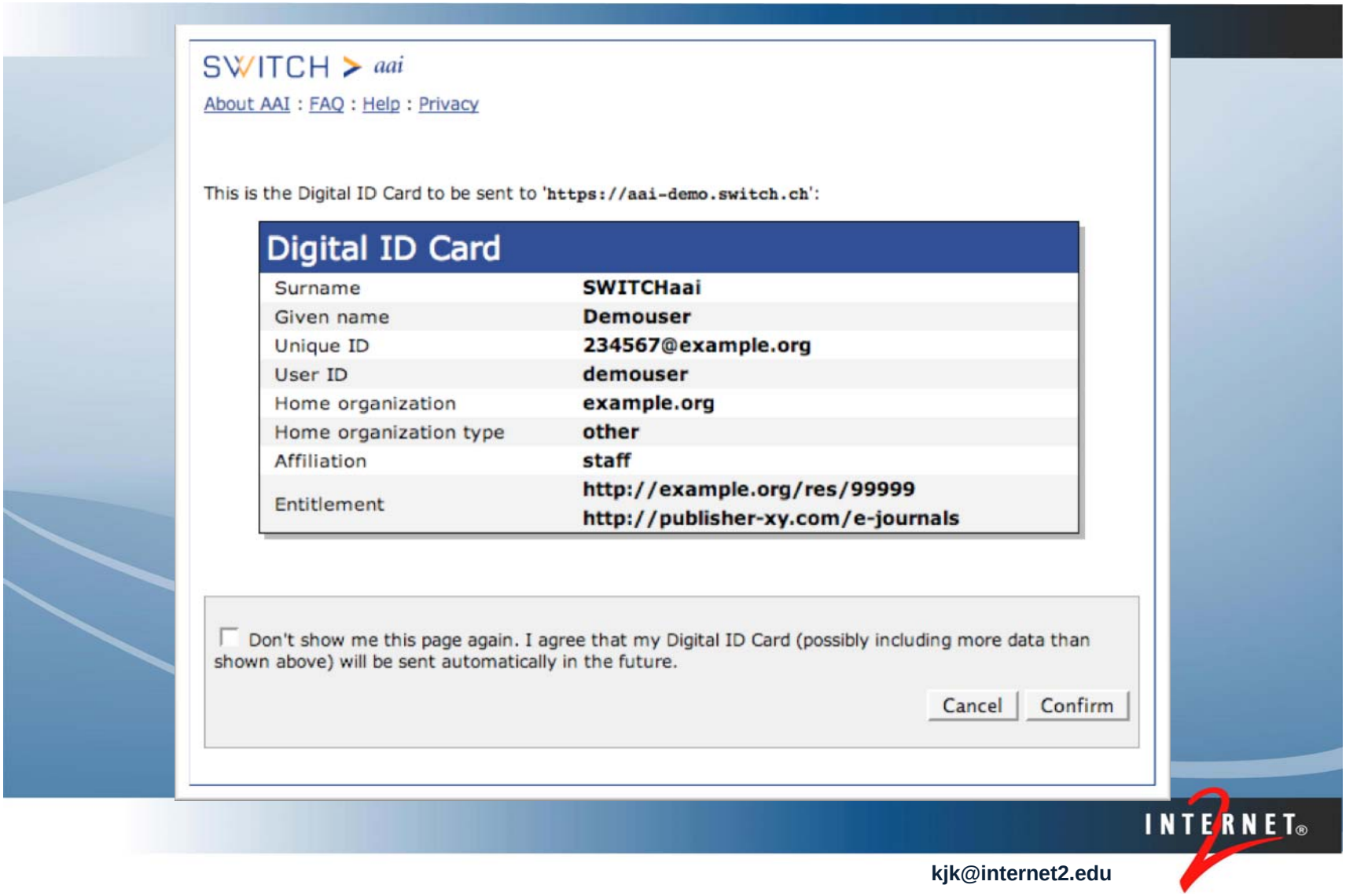
- SAML 2.0 watershed for basic interop
- Key new functionalities such as attribute aggregation, privacy managers, account linking, N-tier, OpenId libraries being added
- Addressing new high-end and new-user requirements

kjk@internet2.edu

Some examples

- Delegated assertions – policy management
- Expanded attribute aggregation
- Simplified configuration, especially for metadata
- More powerful configuration, especially for metadata
- Expose token/signature validation as web services –
  - Plug Shib style trust management into other sustems and implementations

kjk@internet2.edu



kjk@internet2.edu

Grouper

- Simpler UI
- Role management capabilities
- Kuali integration
- uPortal integration
- LDAPPC NG (LDAP NG?)
- https://spaces.internet2.edu/display/GrouperWG/Grouper+Product+Roadmap

kjk@internet2.edu

Privilege management

- Lessons learned
- A variety of steps forward
  - Adding priv man capabilities to Grouper
  - Guides to untangling privilege “snags” and getting a structured campus conversation going
  - Working with open source application projects that have some elements of privilege management to see if they can be extended to broader use cases
  - Campus contributions such as perMIT

kjk@internet2.edu

IdM for Collaboration (COmanage)

- Harnessing Shib, Grouper and priv man together (with some other glue) to support inter-realm collaborations
- Externalizes common IdM from collaboration and domain apps into a coordinated, self-contained but re-plumbable platform
- Delivered as a framework/service/appliance
- An international area of interest and work

kjk@internet2.edu

What is Out of Scope

- ESB, workflow, DRM, etc
- Grid software
- UI design beyond the subject area
- Lots of other stuff…
- The Internet of things

kjk@internet2.edu

Data Standards

- eduPerson refresh
  - Clarity on epTid
  - More semantics ?
  - A few new attributes (eduPersonOpenId?)
- Guidelines on new schema (e.g. NIHextperson, GENI)
- New edu schema if needed

kjk@internet2.edu

InCommon Trust Services

- Develop and deploy core federation
  - Basic, Bronze and Silver
  - Improved metadata services
- Evaluate, develop and deploy related services as appropriate
  - Certificate services
  - Shibboleth training and IdM consulting
  - Outsourced federation operations
  - Eduroam

kjk@internet2.edu

InCommon Silver

- LOA 2 on the campus
- Highly secure federation operational procedures
- Many applications require it (especially with LOA 1 now being soooooo low)
- May enfold other procedures on campuses

kjk@internet2.edu

Possible new services

- Certificate services
  - SSL
  - Root CA (USHER)
  - Personal certs
  - Grid replacement certs

kjk@internet2.edu

eduRoam

- International wireless roaming for the R&E commnity - www.eduroam.org
- 802.1x based authn technology, not web-redirect authn; typically requires client on laptop
- Federation might be the scope of use, types of policies, operator, etc but still not use the web authn that people think of as “federation”.

kjk@internet2.edu

Shib training and IdM consulting

- Intended to accelerate adoption more than generate revenue
- Shib training already a useful service in other countries
- IdM consulting more of a prolonged engagement or self-help groups or …

kjk@internet2.edu

Operating other federations

- Some sectors may need help – K-20, health, etc.
- Could be operational or consultative
- Not an early target of opportunity

kjk@internet2.edu

Some thoughts about the future

- Perilous and uncertain
- Not all businesses enabled by InCommon should be operated by InCommon…
- Tend to the knitting
  - Stick close to core skills and purposes
  - Do a few things well

kjk@internet2.edu