Life on the Exponential: Of the Internet and Internet Identity

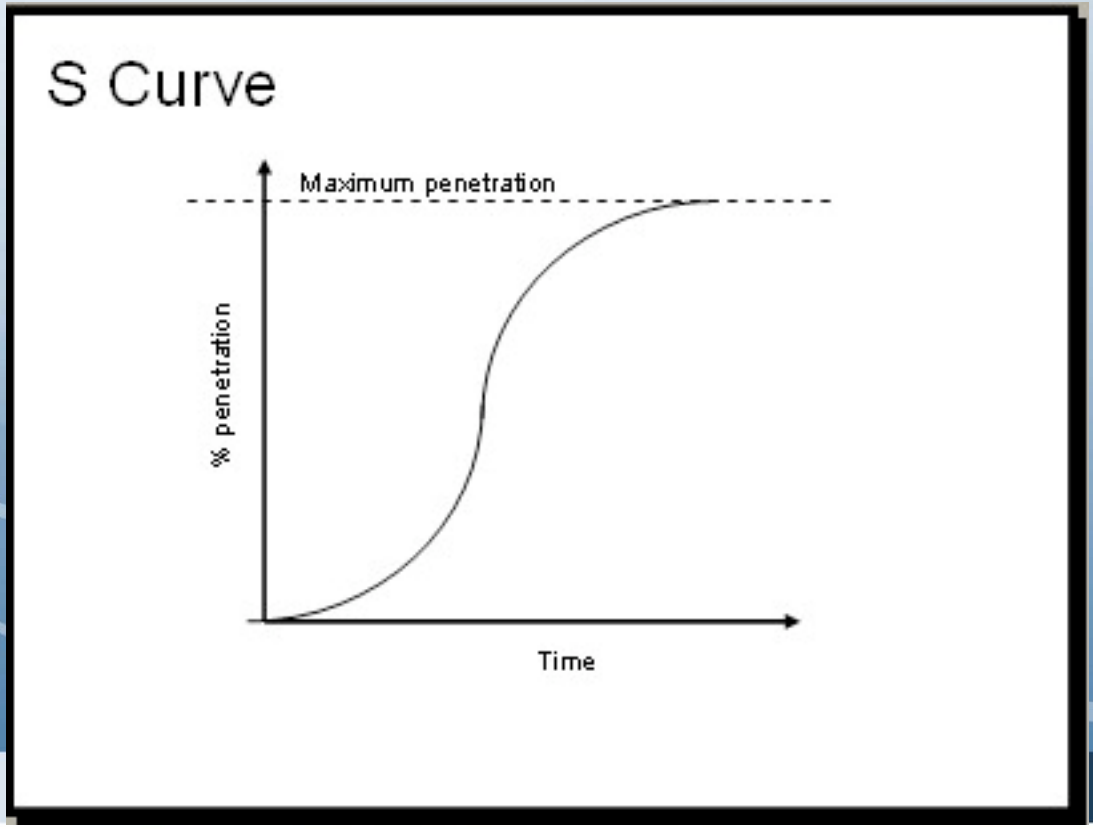
Dr Ken Klingenstein
Director, Internet2 Middleware and Security

INTERNET2®

Topics

- The Rise of the Internet
- The Rise of Internet Identity
- Some things are the same; some are different
- The Role of eScience
- The Role of eGovernment
- What comes Next

The Exponential and S Curve of Technology

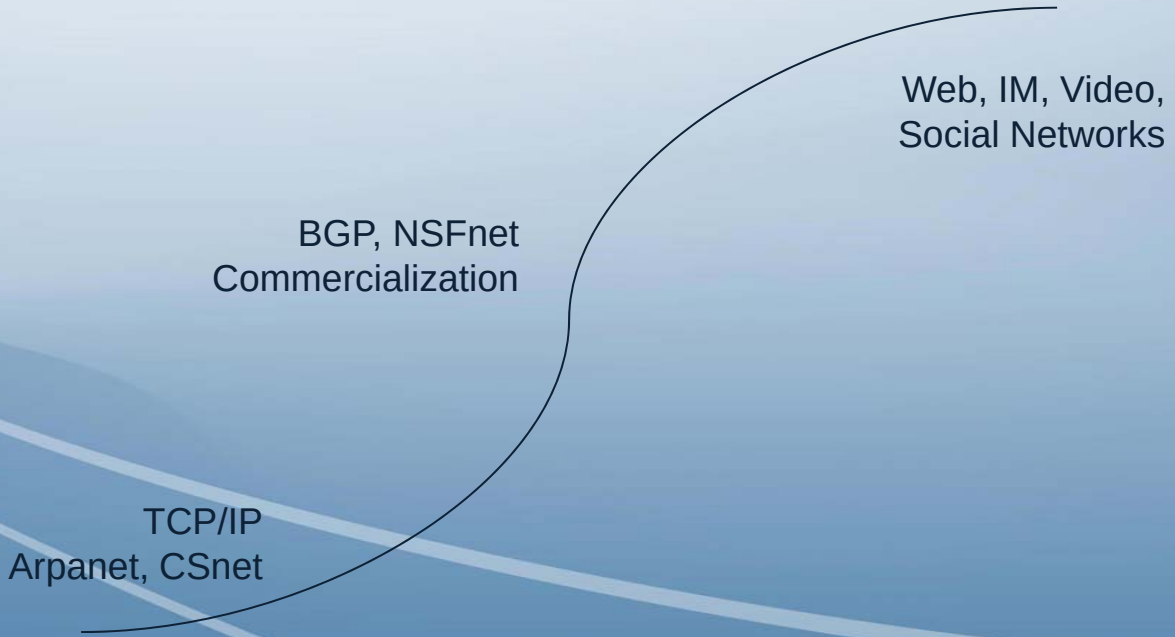


kjk@internet2.edu

The Rise of the Internet

- Making the technology: 1969-1985 - established the core TCP/IP technologies and value to the Computer Science community
- Making the market: 1985-1998, R&E made a mass market of technology, applications and content, using NSFnet, Bitnet, etc
- Making the business: 1998-now - business plans and businesses take a role

The Rise of the Internet



kjk@internet2.edu

The Rise of the Internet

Web, IM, Video,
Social Networks

BGP, NSFnet
Commercialization

TCP/IP
Arpanet, CSnet

1969-1982

1985-2000

2000-2010

kjk@internet2.edu

kjk@internet2.edu

Lessons learned

- Modular and layered design
- A “narrow waist” of technology
- Open standards, open source
- Autonomous systems, loosely coupled
- Network externalities a powerful force
- Most don’t understand at first, and then there is a tipping point and it is obvious to all.

kjk@internet2.edu

The Emergence of Middleware and Internet Identity

- Development of campus and enterprise services common to many applications
  - Directories, enterprise authentication, group and privilege management, identity services, the enterprise service bus, etc…
  - Policies and business processes that drive services
- Federations to extend middleware to interrealm needs
  - Federating software
  - Trust policies
  - Shared attributes

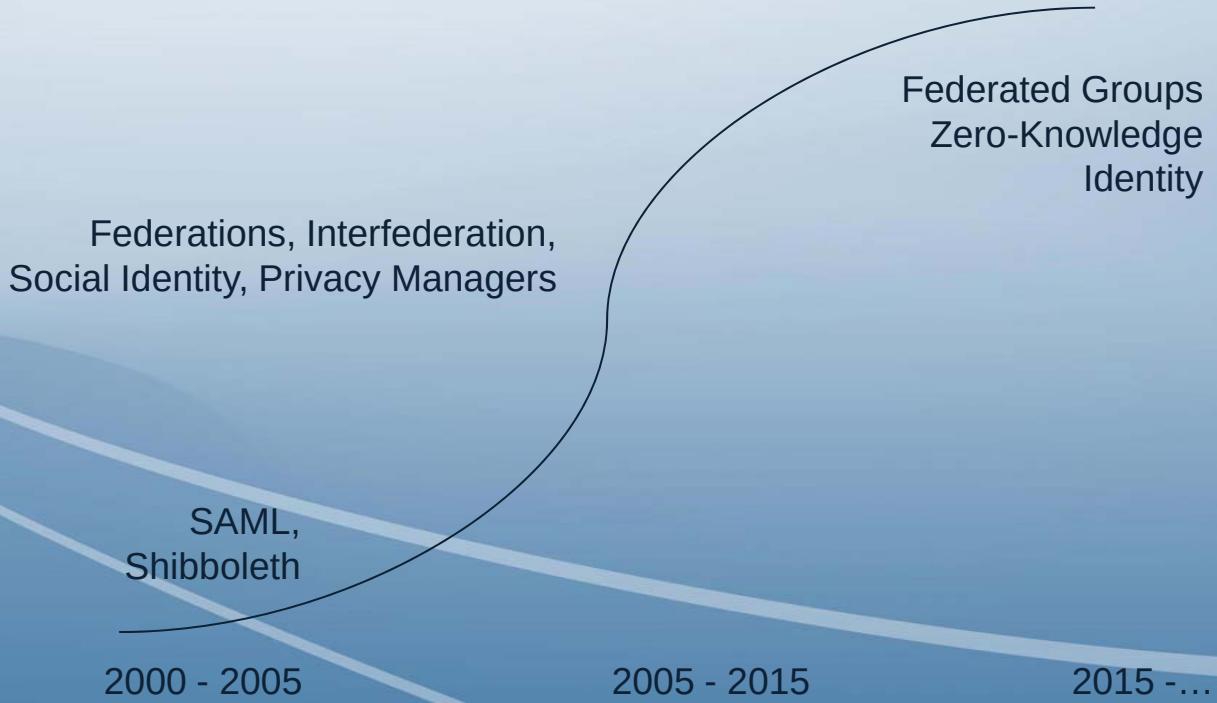
kjk@internet2.edu

Where we are now

- Building an Identity layer for the Internet
  - Identifiers
  - Levels of authentication and assurance
  - User Interface – Discovery, Authentication, Attribute release
- Building an access control layer for the Internet
  - Passing attributes for access control decisions
    - Sometimes the Identity provider decides and passes an entitlement
    - Sometimes the Relying party wants to decide and the Identity provider passes attributes
  - Shared understanding and administration of group management

kjk@internet2.edu

The Rise of Internet Identity



kjk@internet2.edu

The Rise of Internet Identity

Federated Groups
Zero-Knowledge
Identity

Federations, Interfederation,
Social Identity, Privacy Managers

SAML,
Shibboleth

2000 - 2005 2005 - 2015 2015 -…

kjk@internet2.edu

Lessons learned

- Modular and layered design
- A “narrow waist” of technology
- Open standards, open source
- Autonomous systems, loosely coupled
- Network externalities a powerful force
- Most don’t understand at first, and then there is a tipping point and it is obvious to all.

kjk@internet2.edu

Some things the same

- The purpose is to foster collaboration
- The design of the technology – “we saw a different problem and solved it in the obvious way”
- We are not so much different from the corporate world – we just have a more urgent need to collaborate beyond our organizational borders

kjk@internet2.edu

Some things are different

- Policies and practices are a bigger part of the picture
- There is an embedded base of bad solutions
- National boundaries mean more, due to privacy laws

kjk@internet2.edu

R&E Federations

- Substantial deployments in many countries, including UK, Norway, Switzerland, Sweden, Japan, Australia, France, Denmark, Finland, Spain, Germany, Netherlands, etc. Coverage in a number of countries is now 100%.
  - Uses include roaming access, grid credentials, digital content access, wiki controls
- In the US, a national federation – InCommon – and others - Texas (three federations), UCTrust, CalState Trust, Libraries of Florida – Federation Soup

InCommon

- US R&E Federation,
- 200+ members - universities, service providers, government agencies, national labs, 5 M users
- Millions of assertions a day
- Access to controlled wikis, academic content (Elsevier, etc) clouds and Grids, services (student travel, testing, etc), Microsoft, Google Apps for Education, science portals,
- Access to national science resources
- Access to national medical resources and institutes
- Building multiple levels of assurance (LOA)

InCommon LOA

- InCommon – today's federation
- Bronze (LOA 1)- A campus researcher uses their campus account to access an NIH clinical trial wiki
- Silver (LOA 2) – A sponsored research accountant uses their secure campus account to modify documents on NSF Fastlane
- Gold (LOA 3) - A campus security officer could use their local two factor authentication to participate in a Teragrid security incident

Federated Identity Serving eScience

- Domain science
- Grant administration
- Supporting the Virtual Organization (VO)
- Collaboration management platforms

kjk@internet2.edu

Domain Science and Federations

- The Teragrid has go.teragrid.org – a federated login service
- GENI – the NSF advanced networking effort, uses federations of many types
- Scholarly services accessed by federations
  - Publishers
  - Clouds by Microsoft and Amazon
  - Collaboration tools

kjk@internet2.edu

Grant administration

- Grant life-cycle management at NIH and NSF
  - Submission and Review
  - Budgeting
  - Reporting
- Over 30 applications at NIH andhttp://research.gov for NSF

Virtual Organizations

- High-profile individuals doing big science
  - Compute intensive, data intensive, network intensive
- Often international, often expensive shared equipment
- Traditional requirements were command line; new needs are web services
- Need identity and access control

kjk@internet2.edu

LIGO

- Detection and measurement of cosmic gravitational waves
- 750 scientists, researchers and staff across 50 institutions spread over 6 countries
  - ICRR has two laboratories for gravitational wave research, one is Pro.Kuroda lab. and Aso. Pro. Ohashi lab. Both are always collaborating to realize LCGT (Large Scale Cryogenic Laser Interferometer Telescope) project.
  - http://www.icrr.u-tokyo.ac.jp
- Need identity and access controls
  - Domain Science – federated SSH
  - Collaboration – wikis, calendars, versioning systems, etc

Integration of identity and access control

- Identity and access control (groups) need to integrate across three science environments
  - Command-line-managed instruments generate data feeds that populate data bases
  - Using web browsers, scientists access the database, mark events, set data feeds, etc.
  - Other communities come in through science gateways and portals
- Federated identity and domestication of applications is needed

kjk@internet2.edu

Collaboration management

- Providing identity, groups and privileges in a common fashion to a wide variety of applications
- Applications include wikis, lists, code versions systems, file hares, event calendaring, ad hoc calendaring, audioconferencing, etc.
- Can be implemented in several ways
  - a portal
  - COmanage – a stand-alone platform
    - (http://middleware.internet2.edu/co/)
  - As a national collaboration infrastructure
    - http://www.surfnet.nl/Documents/indi-2009-07-020%20(Report%20Collaboration%20Infrastructure).pdf>

kjk@internet2.edu

Early results

- Federated users are much more likely to use shared resources (e.g. wikis, clinical trial data) than users with separate accounts
- Researchers now pushing their campuses into federation
- Help desk calls reduce by 85%
- Federated users ask for more collaboration tools – e.g. ad hoc calendaring, versioning systems

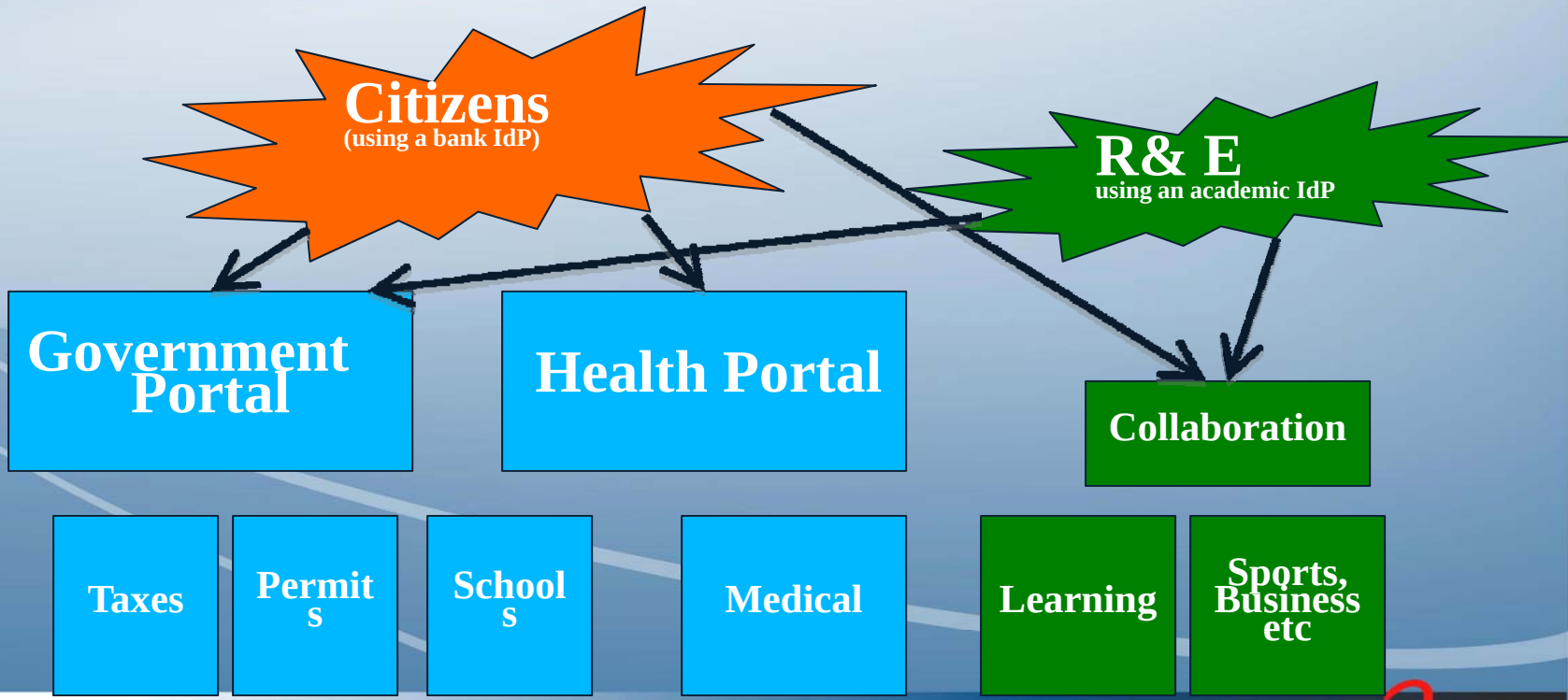
kjk@internet2.edu

Federated Identity Serving eGovernment

- Citizen to government
  - At the national level
  - At the local level
- Business to government
- Government to government
  - Dept of Justice and Department of Defense
  - Among the many parts of Justice

kjk@internet2.edu

Federations and Government in Denmark



kjk@internet2.edu

The “Plan” in the US

- InCommon to access government applications at LOA 1,2, and 3
- Google, Yahoo, AOL, etc to access government applications at LOA 1 using OpenId
- Paypal and Banks may offer accounts as well
- State governments using internal federations

Other E - government instances

- In Norway, most local governments are now joining the R&E federation (Feide) as service providers
- In the Netherlands governments interact with the R&E
- In the UK, the government operates an IdP for citizens to access government services

kjk@internet2.edu

The Texas Lone Ranger in the past

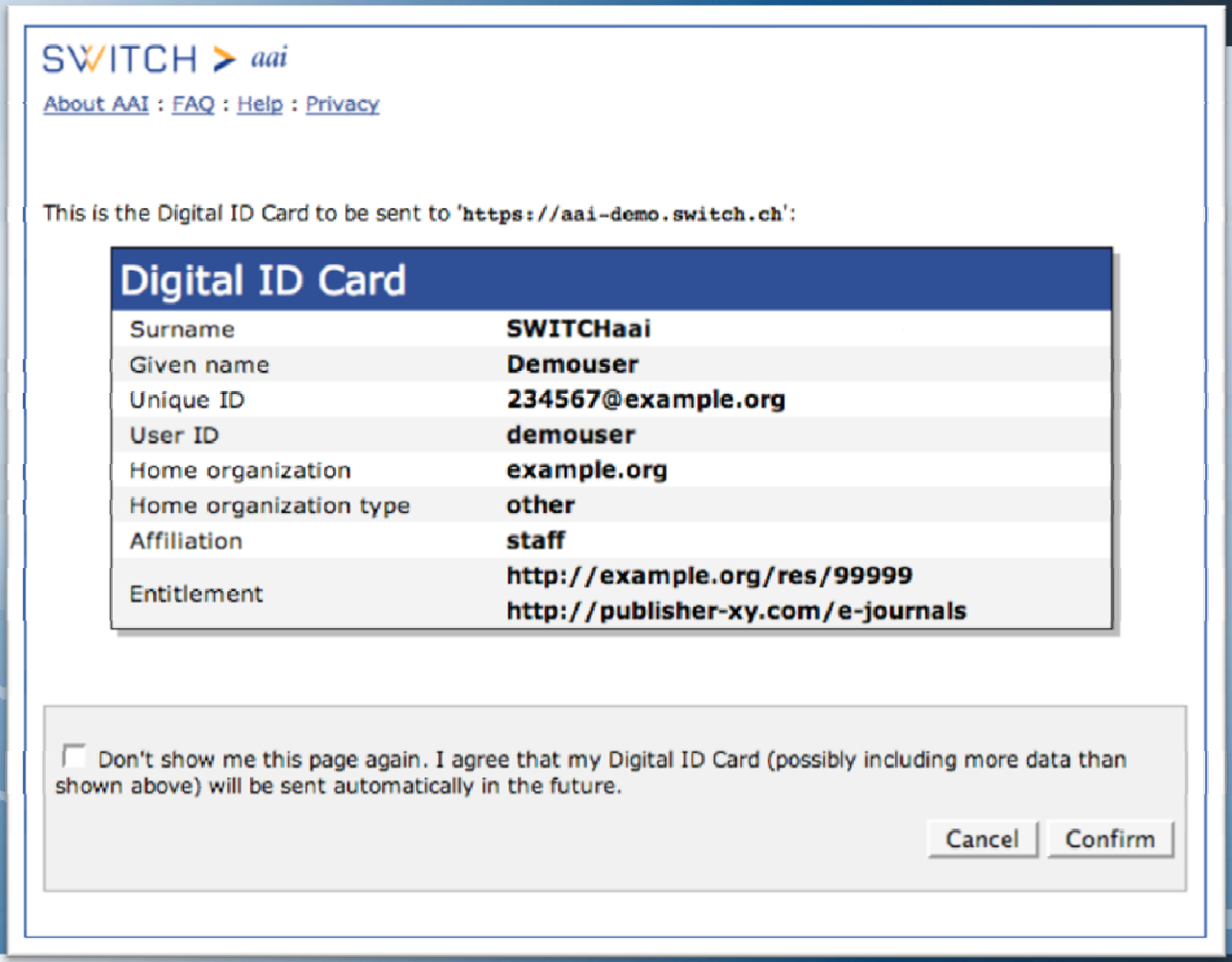
The Texas Rangers now - federated

The Texas Rangers now sit in police cars and use Shibboleth to access state databases

What Comes Next

- User managed attribute release
- Trust Identity and the Internet
- Interfederation
- Collaborations and Virtual Organizations
- Non-web applications
- The Internet of things
- The Attribute Ecosystem and the Tao of Attributes

kjk@internet2.edu


SWITCH aai
About AAI : FAQ : Help : Privacy
This is the Digital ID Card to be sent to 'https://aai-demo.switch.ch':
Digital ID Card
Surname SWITCHaai
Given name Demouser
Unique ID 234567@example.org
User ID demouser
Home organization example.org
Home organization type other
Affiliation staff
Entitlement http://example.org/res/99999
http://publisher-xy.com/e-journals
Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.
Cancel
Confirm

Trust, Identity and the Internet

- The Internet was built for friendly behavior; that is not the current situation
- ISOC initiative to introduce trust and identity-leveraged capabilities to many RFC's and protocols
- http://www.isoc.org/isoc/mission/initiative/trust.shtml
- First target area is DKIM; subsequent targets include SIP and firewall traversal (trust-mediated transparency)

kjk@internet2.edu

Interfederation

- Connecting autonomous federations
- Critical for global scaling, accommodating state and local federations, integration across sectors
- Has technical, financial and policy dimensions
- Elegant technical solution being developed in the eduGAIN project of Geant
- Policy activities in Kalmar2 Union, Geant, Kantara, Terena

kjk@internet2.edu

Non web applications

- Many non-web apps want federated identity – wireless roaming, videoconferencing, soft phones, SSH, Grids, next-generation Internet, calendaring, etc.
- Adding federated authentication and authorization to them is generally engineered on a per case basis.
- Project Moonshot, funded in Europe, looking to work through a general solution by extending IETF protocols

kjk@internet2.edu

The Internet of things

- We have built the Internet of computers and now the Internet of people and identity; next is things.
- Federation is a powerful model – it provides a degree of local freedom but a scalable infrastructure; with interfederation it can reach Internet scale.
- Devices need to have identity, attributes, access control privileges, etc that tend to federate and also need to interact with identity federation.
- Next generation Internet work has many types of federations of circuits, of firewalls, of routers, etc.

kjk@internet2.edu

The Attribute Ecosystem

- Authentication is very important, but identity is just one of many attributes
- And attributes provide scalable access control, privacy, customization, linked identities, federated roles and more
- We now have our first transport mechanisms to move attributes around – SAML and federations
- There will be many sources of attributes, many consumers of attributes, query languages and other transport mechanisms
- Together, this attribute ecosystem is the “access control” layer of infrastructure

kjk@internet2.edu

The Tao of Attributes workshop 属性之道

- Purpose of workshop was to start to explore the federal use case requirements for attributes, aggregation, sources of authority, delegation, query languages, etc.
- Participants were the best and brightest – the folks who invented LDAP, SAML, OpenId, etc.
- Webcast at http://videocast.nih.gov/PastEvents.asp
- Twittered at TAOA
- http://middleware.internet2.edu/tao-of-attributes/

The Exponential is a Good Ride

- Rapid, transformative change
- The curve will start to flatten
- Always unexpected consequences
- A once-in-a-lifetime experience
  - The luck to have had it twice…

kjk@internet2.edu