Eighteenth Federal & Higher Education PKI Coordination Meeting (Fed/Ed XVIII)
Friday, December 12, 2008 — 10am-4pm
EDUCAUSE Office, 1150 18th Street, NW, Suite 1010, Washington, DC
Sponsored by EDUCAUSE

Registration List

On Site

Bill Altmire, NSF
Chen Arbel, Aladdin
Ardoth Hassler, NSF
Scott Rea, Dartmouth College
Gary Secrest, Johnson & Johnson

Michael Sessa, PESC
Mollie Shields-Uehling, SAFE Bio-Pharma
Judy Spencer, FICC
David Temoshok, GSA
Steve Worona, EDUCAUSE

By Phone

Debb Blanchard, CyberTrust
Paul Caskey, University of Texas System
Nick Davis, U of Wisconsin-Madison
John Harris, Adobe
Wes Hubert, University of Kansas
Ken Klingenstein, Internet2

Clifton Leonard, University of Oklahoma
Valerie Vogel, EDUCAUSE
David Wasley, Internet2/EDUCAUSE
Bill Weems, UTHSC-Houston
Ann West, Internet2/EDUCAUSE
Mary Fran Yafchak, SURA

Tentative Speaker Slots
(others as time and interest permits)

Before Lunch

Ann West
Judy Spencer
Scott Rea
Ken Klingenstein
Ardoth Hassler

During/After Lunch

Paul Caskey
Mary Fran Yafchak
David Temoshok
Nick Davis
Michael Sessa
Wes Hubert
John Harris
Gary Secrest
Mollie Shields-Uehling

Mark Your Calendar

Nineteenth Federal & Higher Education PKI Coordination Meeting (Fed/Ed XIX)
scheduled (tentatively) for
Thursday, June 11, 2009
10am-4pm

Location

EDUCAUSE Office: 1150 18th Street, NW, Suite 1010
Quick Background

- 2004 UW-Madison purchased co-managed solution from Geotrust
- Both client certs and SSL certs are purchased from Geotrust
- Started September, 2004
- Centrally funded
Current Environment

- Over 1000 client certs currently in use across campus
- Used for email signing, document signing and encryption
- Documents, PDF, Word, multiple email clients
- We hosted the First Annual Educause PKI Deployment Forum in April, 2008.
New Use for Certificates at UW

- Dual factor authentication to protect sensitive web applications
- Web Initial Sign-on Client based on Pubcookie
- Altered to authenticate via digital certificates
Where are the Certificates Stored?

- Etokens, local drives
- HID Crescendo Cards
- New UW-Madison ID cards contain: magnetic stripe, bar code, printed number, picture, status (staff/student), 2 RFID cores (Prox and iClass)
- Subset of cards (250) contain the HID Crescendo chipset
• Crescendo chipset
• Raaksign software
• Windows only software included, Macintosh 3rd party software available
• Design story
McAfee Safeboot

- Whole disk encryption being deployed on a volunteer basis
- Can use certificates in pre-boot authentication
- HID Crescendo card is supported by McAfee for pre-boot authentication
PKI Rollout to UW-System

- UW System plans to roll digital certificates out across UW statewide system
- 26 campuses
- Prime driver is encrypting sensitive email and digital signing of mass email
- 56,000 person signed email sent this week
Issues With Mass Email

• Too complex for some people to figure out
• Some people agree to delegate signing authority
• Is it ideal? No
• Does it get the job done? Yes
Our Guiding Principles

- Keep it simple
- Balance ideal security with the needs of our user community
- Make it usable outside of our campus
- Coolness factor, can’t be underestimated. The unified card is a big hit!
Next Steps

- Put our PKI contract out for bid
- Geotrust absorbed by Verisign, True Credentials no longer being actively promoted or developed
Questions

• Questions and comments welcome at this time, EXCEPT for questions from Scott Rea!

Nicholas Davis
ndavis1@wisc.edu
InCommon@NSF

Bill Altmire  
Acting Branch Chief for the Telecommunications Branch  
Project Leader, eAuthentication

Ardoth Hassler  
Senior Information Technology Advisor &  
Associate Vice President for University Information Services  
Georgetown University

December 12, 2008
NSF is joining InCommon

- **Status:**
  - Agreement
    - reviewed
    - Pending final approval and signatures
  - Ready to begin testing

- Functionality demonstrated with FastLane at Internet2
What will our customers be able to do?

- **Research.gov**
  - View Proposals
    - NSF and USDA/CSREES – today
    - Army Research Office – December 2008
    - More in progress
  - Login with credentials issued by their home institution (Bronze)
  - Create and submit Federal Financial Reports to NSF
  - Maintain their user profiles
  - And much more…

- **FastLane**
  - Login with credentials issued by their home institution (Bronze)
  - Access and use current PI/co-PI suite of functions
  - Perform Research Administration
  - Use proposal and award functions
Visit www.Research.gov
Implementation Plans

• Start with a pilot program:
  – Connect Research.gov with
    • University of California-Davis
    • Colorado State University
    • Georgetown University
    • Pennsylvania State University
    • University of Washington
  – Have available as Research.gov functionality enhances

• Add FastLane next
  • Timing: TBD
NSF Large Facilities Are Already Joining InCommon

Ocean Observatories Initiative
- In progress

TeraGrid
- piloting/testbed now
  - Expect XD (TG phase 3) to use it in production

Laser Interferometer Gravitational-Wave Observatory
- In progress
Fed-Ed Dec 08: Updates on Federations

Dr. Ken Klingenstein, Senior Director, Middleware and Security, Internet2 Technologist, University of Colorado at Boulder
Topics

• Internet identity update
  • Technology updates
  • ISOC, IETF “Identity, Trust and the Internet”
  • Privacy and its implications for federation
• Federations
  • US
    • InCommon and Soup
    • Planning the future of InCommon
  • Liberty Alliance, International
• Applications update
  • Collaboration apps
  • Open source kumbaya
Internet identity

• Federated identity
  • Enterprise centric, exponentially growing, privacy preserving, rich attribute mechanisms
  • Requires lawyers, infrastructure, etc
• User centric identity
  • P2P, rapidly growing, light-weight
  • Marketplace is fractured; products are getting heavier to deal with privacy, attributes, etc.
• Unifying layers emerging – Cardspace, Higgins
Federated identity

• Convergence around SAML 2.0 – even MS
• Exponential growth in national and international R&E sectors
• Emerging verticals in the automobile industry, real-estate, government, medical
• Policy convergence for LOA, basic attributes (eduPerson), but all else, including interfederation, remains to be developed
• Application use growing steadily
• Visibility is about to increase significantly through end-user interactions with identity selectors and privacy managers

kjk@internet2.edu
User-centric identity

- Driven by social networking {Facebook, MySpace, etc} and {Google, AOL, MSN}, growing rapidly
- Relatively lightweight to implement for both application developers and identity providers
- Separates unique identifier and trust (reputation systems, etc.)
- Fractured by lack of standards, vying corporate interests, lack of relying parties, etc.
- OpenId, Facebook Connect, Google Connect, AOL
Unifying the user experience

- Among various identity providers, including P2P, self-issued, federated
- Need to manage discovery, authentication, and attribute release
- Cardspace, Higgins, uApprove, etc.
- Consistent metaphors, somewhat different technical approaches
- Starting to deploy
- Integrating enterprise and social identity
Trust, Identity and the Internet

• ISOC initiative to introduce trust and identity-leveraged capabilities to many RFC’s and protocols
• Acknowledges the assumptions of the original protocols about the fine nature of our friends on the Internet and the subsequent realities
• First target area is DKIM; subsequent targets include SIP and firewall traversal
Privacy

• A broad and complex term, like security, encompassing many different themes
• An important privacy issue - personal data release
  • What is personal data?
  • Release a function of national, EU, and local policy
  • International transactions common and complex
  • Roughly separates into “required for transaction” and “needs consent”
EU Privacy Laws

• Art 29 WG overarching but lots of confusion below
• IP address
• EPTID – a non-correlating, opaque but persistent identifier
  • For privacy and state – e.g. searches, web blogs
  • Critical to federated privacy
Some UK – EU recommendations

Identity Providers should

• Construct pseudonymous identifier values in ways that conceal as far as possible the identity of the user, for example by using one-way hash functions and providing different values to each service provider;

• Declare that they will not disclose the identity of the person to which a particular identifier value was assigned, other than when required by law to do so.

• In particular, reports of misuse or other problems should be investigated by the Identity Provider, who is anyway most likely to be able to hold the user to account, and not the Service Provider.

Service Providers should

• Not collect personally identifying information from a user who was otherwise only identified by a pseudonymous identifier;

• Not seek to obtain information linking a pseudonymous identifier to a user from any other source; in particular they should not aggregate information collected from different services;

• Provide evidence to Identity Providers to permit them to investigate and deal with any misuse or other problem in the use of the service.
Federation Update

• R&E federations sprouting at national, state, regional, university system, library alliance, and elsewhere

• Federated identity growing in business
  • Many bilateral outsourced relationships
  • Hub and spoke
  • Multilateral relationships growing in some verticals

kjk@internet2.edu
R&E Federation Killer Apps

- Content access – Elsevier, OCLC, JSTOR, iTunes
- Government access – NIH ERA, CTSA, soon NSF and research.gov
- Access to collaboration tools – wikis, moodle, foodle
- Roaming network access
- Outsourced services – National Student Clearing House, student travel, plagiarism, testing, travel accounting
- MS Dreamspark
InCommon

- Over 118 members and growing steadily
- More than two million “users”
- Most of the major research institutions
- New types of members
  - Non usual suspects – Lafayette, NITLE, Univ of Mary Washington, etc.
  - National Institute of Health, soon NSF and research.gov
  - Energy Labs, ESnet, TeraGrid
  - MS, Apple, Elsevier, etc.
  - Student service providers
- Steering Committee chaired by Clair Goldsmith of Univ of Texas;
  Technical Committee chaired by Renee Shuey of Penn State
InCommon Update

• Growth is quite strong; doubled in size for the fifth year straight…
• Potential size estimates (pre-interfederation) could grow > 5,000 enterprises; revenue stream….
• Overarching MoU for federal agencies to join may happen
• Silver profile approved
• Major planning effort on the future of InCommon now underway, including governance, community served, pricing and packaging principles, business models
Grist for InCommon direction setting

- Comparison to other national R&E federations
- Budget, basics
- Strength-weakness-opportunities-threats analysis
- Status of soup
- Growth and expense/revenue projections
  - Effect of interfederation and soup on projections
- Other business opportunities

kjk@internet2.edu
Principles to be established by process

• Community served
• Business opportunities
• Governance and representation
• Pricing and packaging principles – membership models, working with soup, etc.
• Charge by cost or charge by value

• The relationship between InCommon and Internet2
Federation Soup

• Within the US, federations happening in many ways – state, university system, library, regional, etc
• Until we do interfederation, and probably afterwards, federations will form among enterprises that need to collaborate, regardless of their sector
• Common issues include business models, legal models, LOA and attributes, sustainability of soup
• Overlapping memberships and policy differences creates lots of complexity in user experience, membership models, business models, etc.
• One workshop in, so far…
• https://spaces.internet2.edu/display/FederationSoup/Home
Liberty Alliance

• A locus for federation discussions
  • eGov
  • IAAF
  • New Interfed SIG soon to start
    • Dealing with policy aspects of Interfed
    • Reaching out across sectors
• Trying to walk the walk as well – multifederated wiki for discussions

kjk@internet2.edu
International federations

- More than 25 national federations;
- Several countries at 100% coverage, including Norway, Switzerland, Finland; communities served varies somewhat by country, but all are multi-application and include HE
- UK intends a single federation for HE and Further Education ~ tens of millions of users
- EU-wide identity effort now rolling out - IDABC and the Stork Project (www.eid-stork.eu)
- Key issues around EU Privacy and the EPTID
- Some interfederation – Kalmar Union and US-UK
REfeds meeting

• Utrecht Dec 4-5
• All federations reporting tipping point phenomena
• Key issues include building the business, communities served, attribute development, interfederation, application integration, working with Liberty Alliance, international privacy, etc
• Integration with e-Science, CLARIN, etc.
• http://www.terena.org/activities/tf-emc2/meetings/12/index.html
Next Steps for the R&E federation community

• Learning the business of federation - REfeds
• Attributes redux - ?
• LOA – Liberty IAAF
• Application enablement – MACE, TF-EMC2, etc
• Short-term metadata aggregation -?
• Long-term dynamic metadata development – EMC2
• EGov – Liberty eGov SIG
• Support of virtual organizations and collaborations - REfeds
• Outreach to emerging R&E feds – REfeds
• Outreach to other sectors - Liberty

kjk@internet2.edu
More next steps

- Federated operator practices standards – Liberty (but where)
- Common member-federated operator agreement – IETF/ISOC
- Common member operational practices statement – IETF/ISOC
- Interfederation – Liberty Interfed SIG
- Technical common standards – EMC2
  - Attribute mapping, attributes into English, standard approaches to InfoCard, uApprove, etc.
Collaboration and Federated Identity

• Two powerful forces being leveraged
  • the rise of federated identity
  • the bloom in collaboration tools, most particularly in the Web 2.0 space but including file shares, email list procs, etc
• Collaboration management platforms provide identity services to “domesticated” applications that externalize their identity management dimensions to an general identity/group/privilege/etc repository (LDAP, MySQL, etc.)
• Results in user and collaboration centric identity, not tool-based identity
• COmanage is a collaboration management platform, supported in part by a NSF OCI grant, being developed by the Internet2 community, with Stanford as a lead institution
COmanage

- COmanage can provide authentication and authorization services (group membership, privilege management, etc) to apps
- Domesticated applications currently include wiki, listproc, Jira, Subversion, Al Fresco. Soon to add audioconferencing, IM and chat rooms, EC2, Fedora, web-based file share, etc.
- Can be launched as an image in the Amazon cloud.
- Not “collaboration in a box”. More collaboration in a fully permeable membrane. The “stand-alone” can be readily replumbed to be completely integrated into enterprise, federated or other attribute ecosystems as they develop
- Uses Shibboleth and Grouper and…
Integration with Open Source Efforts

- Federated versions of Fedora and DSpace abound; domesticated versions to come
- Sakai, Moodle, etc also federated
- Kuali and Rice/KIM are under active discussion
- Asterisk, Openwiki, other collaboration tools
Creating Silos of Trust
LOA: Levels of Assurance

• Not all CAs are created equal
  – Policies adhered to vary in detail and strength
  – Protection of private keys
  – Controls around private key operations
  – Separation of duties
  – Trustworthiness of Operators
  – Auditability
  – Authentication of end entities
  – Frequency of revocation updates
HEBCA : Higher Education Bridge Certificate Authority

- Bridge Certificate Authority for US Higher Education
- Modeled on FBCA
- Provides cross-certification between the subscribing institution and the HEBCA root CA
- Flexible policy implementations through the mapping process
- The HEBCA root CA and infrastructure hosted at Dartmouth College
- Facilitates inter-institutional trust between participating schools
- Facilitates inter-federation trust between US Higher Education community and external entities
HEBCA

• What is the value presented by this initiative?
  – HEBCA facilitates a trust fabric across all of US Higher Education so that credentials issued by participating institutions can be used (and trusted) globally e.g. signed and/or encrypted email, digitally signed documents (paperless office), etc can all be trusted inter-institutionally and not just intra-institutionally
  – Extensions to the Higher Education trust infrastructure into external federations is also possible and proof of concept work with the FBCA (via BCA cross-certification) has demonstrated this inter-federation trust extension
  – Single credential accepted globally
  – Potential for stronger authentication and possibly authorization of participants in grid based applications
  – Contributions provided to the Path Validation and Path Discovery development efforts
Solving Silos of Trust
TAGPMA Bridge Working Group

- Recognition that there are different LOAs
  - in the way some credential service providers operate
  - Required by different applications
- More efficient ways of distributing Trust Anchors
- Interoperation with other trust federations
Proposed Inter-federations

- FBCA
- NIH
- CA-1
- CA-2
- CA-n
- Cross-certs

HEBCA
- HE BR
- HE JP
- Cross-certs

Dartmouth
- Texas
- UVA
- Univ-N
- USHER
- C-4
- Cross-certs

CA-1
- CA-2
- CA-3
- CA-4

AusCert CAUDET PKI

CertiPath
- SAFE
- Other Bridges

DST ACES

SAFE
- Other Bridges

SAFE
- Other Bridges

SAFE
- Other Bridges

SAFE
- Other Bridges

SAFE
- Other Bridges
For More Information

• HEBCA Website:
  
  [http://webteam.educause.edu/hebca/](http://webteam.educause.edu/hebca/)
  
Scott Rea - [Scott.Rea@dartmouth.edu](mailto:Scott.Rea@dartmouth.edu)
SAFE-BioPharma Digital Identity and Signature Standard and Services

Fed/Ed XVIII
Friday, December 12th, 2008
SAFE-BioPharma Digital Identity and Signature Standard and Services

- Strategic initiative started 11/03 by biopharmaceutical industry to facilitate transformation to fully electronic

- SAFE-BioPharma Association incorporated May 2005
  - Member-governed, non-profit collaborative industry org
  - Develop and maintain standard
  - Facilitate adoption
  - Services for Members
    - Outreach to regulators
    - SAFE-BioPharma Bridge
    - Tiered Services
    - Commercial issuers/products
    - Cross Certification with FBCA
    - Pilots; new use cases
    - Best practices; industry sharing
SAFE-BioPharma Members

- Abbott
- AstraZeneca*
- BristolMyers Squibb*
- Eli Lilly
- GlaxoSmithKline*
- J&J*
- Merck*
- National Notary Assn.
- Organon-ScheringPlough*
- Pfizer*
- P&G*
- Roche
- Sanofi-Aventis*

*Board and PAA Members
# SAFE Vendor Community

<table>
<thead>
<tr>
<th>SAFE Vendor Partners</th>
<th>SAFE Issuers</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Adobe*</td>
<td>✓ BMS</td>
</tr>
<tr>
<td>✓ Aladdin*</td>
<td>✓ Chosen Security</td>
</tr>
<tr>
<td>✓ Arcot</td>
<td>✓ Citibank</td>
</tr>
<tr>
<td>✓ ARX *</td>
<td>✓ Verizon Business</td>
</tr>
<tr>
<td>✓ Gemalto</td>
<td>✓ IdenTrust</td>
</tr>
<tr>
<td>✓ Gemini Security</td>
<td>✓ J&amp;J</td>
</tr>
<tr>
<td>✓ IBM</td>
<td>✓ TransSped</td>
</tr>
<tr>
<td>✓ IDBS</td>
<td></td>
</tr>
<tr>
<td>✓ Microsoft</td>
<td></td>
</tr>
<tr>
<td>✓ MXI Security*</td>
<td></td>
</tr>
<tr>
<td>✓ Northrop Grumman</td>
<td></td>
</tr>
<tr>
<td>✓ nCipher</td>
<td></td>
</tr>
<tr>
<td>✓ Open Text</td>
<td></td>
</tr>
<tr>
<td>✓ SAIC</td>
<td></td>
</tr>
<tr>
<td>✓ Tricipher*</td>
<td></td>
</tr>
<tr>
<td>✓ Xyzmo*</td>
<td></td>
</tr>
</tbody>
</table>

*SAFE-BioPharma certified products
The Contract-Based SAFE-BioPharma Standard

Business
- Operating Policies
- Contracts
- Processes

- Accept digitally signed transactions
- Agree to limited liability caps
- Agree to dispute resolution
- Agree to identity assurance
- Agree to self-audit & meet SAFE requirements

Technical & Identity
- Certificate Policy (PKI)
- Specifications
- Guidelines

- Identity verification
- Manage identity life cycle
- Comply with referenced standards
- Follow security, audit & control requirements
- Certification
High-Level Architecture

SAFE Bridge CA

Federal Bridge CA

Member A

Member B

SAFE-BioPharma

TransSped

Network Hosted Credentials

Basic Assurance Software

Medium Assurance Software

IdenTrust

cybertrust

FDA

USPTO

Raytheon

Northrop Grumman

Lockheed Martin

CRIIX

Bristol-Myers Squibb

Medium Assurance Hardware

Lockheed

Martin
Member Public Key Infrastructure Options

- **Internal infrastructure**
  - Cross certified with SAFE Bridge
  - BMS, J&J – soon others

- **Outsourced infrastructure**
  - Cross-certified with SAFE Bridge:
    - Chosen Security
    - Citibank
    - IdenTrust
    - TransSped
    - Verizon Business/Cybertrust

- **SAFE tiered services infrastructure (member-funded)**
  - External partners
  - Regulatory uses
  - Healthcare providers
  - Members
Options for Flexible Use

- **Two levels of trust:**
  - Basic Assurance for authentication
  - Medium Assurance for trusted identity uniquely linked to digital signature and EU-qualified

- **Three digital signing technologies:**
  - Software
  - Hardware (zero footprint now undergoing FIPS certification)
  - Roaming

- **Three identity-proofing options**
  - Antecedent – enterprise and on-line
  - Trusted agent
  - Notary – including office/home notary services
On-Line Antecedent Data Sources

- US only at present – international sources being identified
- Based on previous F2F; publicly available data
- Authoritative Antecedent Data sources (e.g., state licensing authorities):
  - DEA Licenses
  - Medical Professional Licenses
    - Physicians & Surgeons
    - Osteopaths
    - Physician Assistants
    - Nursing
    - Pharmacists
    - Among others
  - State Motor Vehicle Records
    - DMV
    - Registrations
  - Property Records
  - Financial/credit records
On-Line Antecedent Process

ID Vetting Successful:
- Applicant Passes 3rd Party Antecedent identity proofing
- Moved to RA queue for processing and Certificate Issuance steps.
- It’s a matter of minutes end-to-end.

ID Vetting Not Successful:
- Unable to verify identity via 3rd Party Antecedent
- Process reverts to Notary Process with two service options:
  - User locates notary
  - RAS/NNA will have a local notary contact the Applicant directly
SAFE-BioPharma and Regulators

» FDA engagement since inception – helped write standard
  - Familiarization program and compliance matrix
  - FDA Statement acknowledging use of SAFE-BioPharma digital signature as facilitating compliance with 21CFR11
  - SAFE-BioPharma members have submitted 1,000s of fully electronic submissions since Sept. ‘06

» EMEA engagement since inception – helped write standard
  - Evaluation, pilots, electronic submission guidance
  - EMEA will use SAFE-BioPharma as access solution to EudraVigilance data base (~3,000 users)
  - 1Q09 eCTD Pilot
### SAFE-BioPharma Pilots & Implementations

<table>
<thead>
<tr>
<th>Organization</th>
<th>Pilots and Implementations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbott</td>
<td>ELN</td>
</tr>
<tr>
<td>Amgen</td>
<td>Clinical Research Info Exchange (CRIX); ELN</td>
</tr>
<tr>
<td>AstraZeneca</td>
<td>eSubmissions (US); ELN; Investigator Portal; Global infrastructure</td>
</tr>
<tr>
<td>BMS</td>
<td>ELNs; Promotional material review (EU); eSubmissions; alliances</td>
</tr>
<tr>
<td>CDC-MedNet-SAFE-SAIC</td>
<td>Cross-jurisdictional public health-disease surveillance</td>
</tr>
<tr>
<td>EMEA</td>
<td>EudraVigilance; eCTDs, regulatory submissions</td>
</tr>
<tr>
<td>GSK</td>
<td>eSubmissions, R&amp;D docs; Global infrastructure</td>
</tr>
<tr>
<td>J&amp;J</td>
<td>90,000+ employees; eSubs; External partners; Records</td>
</tr>
<tr>
<td>Eli Lilly</td>
<td>eSubmissions</td>
</tr>
<tr>
<td>National Notary Association</td>
<td>Digital Notary Signature</td>
</tr>
<tr>
<td>Pfizer</td>
<td>ELNs; eSubmissions; contracts/SOWs; investigator portal</td>
</tr>
<tr>
<td>P&amp;G</td>
<td>ELNs; contracts; HR</td>
</tr>
<tr>
<td>Group Purchasing Org.</td>
<td>Supplier and member contracts</td>
</tr>
<tr>
<td>Sanofi-Aventis</td>
<td>eSubmissions; ELNs; Finance and Purchasing</td>
</tr>
</tbody>
</table>
The Infrastructure and the Network Are In-Place

- **Expanded Communities of Trust – 4BF (4 Bridges Forum) for Collaboration**
  - Federal Bridge CA; Certipath (Defense & Aerospace); Higher Education Bridge CA; SAFE-BioPharma CA
  - Raise awareness
  - Drive use of network of interoperable trusted communities

- **CDC Cross-Jurisdictional Public Health Surveillance Pilot**
  - MN public health; Duluth hospitals and physicians; CDC

- **Group Purchasing Organizations (GPOs)**
  - Hospital systems
  - Suppliers

- **Federation pilot**
Local Public Health Officials

Alert Notification

Internet

Public Health Disease Investigation Portal (Pilot)

Alert Subscription/Notification Service

Disease Investigation Service

NHIN Gateway Service

Clinical Labs

Patient Test Results

ELR System

Notification w/ Lab test results

Patient Test Results

1/20/2009
Please visit the SAFE-BioPharma website: http://safe-biopharma.org/


Learn more about the SAFE-BioPharma Implementation Toolkit: http://safe-biopharma.org/index.php?option=com_content&task=view&id=254&Itemid=422

Watch the SAFE-BioPharma introductory video: http://www.phillipsvideopost.com/safe

Contact us for more information:

Mollie Shields Uehling
CEO
mollie@safe-biopharma.org
(201) 292-1861
(201) 925-2173 (cell) 8621

John Hendrix
Program Director
JHendrix@safe-biopharma.org
(973) 272-

Jon Schoonmaker
Chief of Operations & Technical Program
(301) 610-6060
jon.schoonmaker@safe-biopharma.org

Cindy Cullen
CTO
cindy.cullen@bms.com
(609) 818 4152

Kevin Chisholm, Admin.
Kevin.Chisholm@SAFE-BioPHarma.org
(201) 292-1860

Rich Furr
Head, Reg. Afrs.
RFurr@SAFE-BioPharma.org
(610) 252-5922

Tanya Newton
Manager, Reg Afrs
(908) 213-1069
tanya.newton@safe-biopharma.org

Jon Schoonmaker
Chief of Operations & Technical Program
(301) 610-6060
jon.schoonmaker@safe-biopharma.org

Kevin Chisholm, Admin.
Kevin.Chisholm@SAFE-BioPHarma.org
(201) 292-1860

Rich Furr
Head, Reg. Afrs.
RFurr@SAFE-BioPharma.org
(610) 252-5922

Tanya Newton
Manager, Reg Afrs
(908) 213-1069
tanya.newton@safe-biopharma.org
InCommon Collaboration
Activities: New Partners

Ann West
December 12, 2008
New Partners

• StateNets and Higher Education Systems
• Student Services Providers
New Partners: State, Region, and Consortia

- Increased need for on-line interaction
  - Administrative
  - Teaching/learning
  - Research
- Collaborations with diverse audiences: K12, State government, non-profit/corporate partners, education
New Partners: State, Region, and Consortia

• Questions
  • What does a federation look like?
  • How does one make the value proposition?
  • Who should be included?
  • Should we build on InCommon or build our own?
  • How can one achieve inter-federation interoperability?
New Partners: State, Region, and Consortia

- StateNets and Higher Education Systems collaboration activity
  - Exploring issues relating to building federations
  - Sharing experiences and identifying solutions
  - Build on strategies used by state university systems
  - Culling emerging practices
New Partners: State, Region, and Consortia

• Sponsored by Internet2, EDUCAUSE, and InCommon Federation
• George Laskaris, Co Chair
  • Executive Director of NJEdge
• Wiki - spaces.internet2.edu/display/USFederations/Building+Identity+Trust+Federations
Federated Student Services

• National Student Clearinghouse joined InCommon Federation
  • Piloting access with Stanford
    • Student now
    • Staff in process
  • Recent levels of assurance (LoA) requirements
Federated Student Services: Pilot

- Informing the standards process
- Student and organizational identifiers
  - eduPerson schema
  - AACRAO/PESC data definitions
Federated Student Services: LoA

- NSC’s Student Electronic Access Agreement for Educational Institutions
  - New requirements for access to Student Self-Service applications
    - Refers to NIST LoA 1
  - Optional Addendum for Meteor Real-Time Loan Access
    - Refers to NIST LoA 2
- Opportunity for education
Federated Student Services

• For more on both issues:
  • InCommon Student collaboration group
  • spaces.internet2.edu/display/InCCollaborate/InC-Student
Contact

- Ann West
  - Support outreach and education on identity management issues for Internet2, EDUCAUSE, and the InCommon Federation
    - awest@internet2.edu
    - awest@educause.edu
Southeastern Universities Research Association (SURA) - Intro for Fed/Ed 18

Mary Fran Yafchak
Senior Program Manager, IT
maryfran@sura.org
SURA Mission

SURA is a 501(c)3 university association with 63 member institutions whose mission is to:

- Foster excellence in scientific research
- Strengthen the scientific and technical capabilities of the nation and the Southeast
- Provide outstanding training opportunities for the next generation of scientists and engineers
SURA Region

- 37% of the US population
- 10 EPSCoR states
- 95% of the nation’s Historically Black Colleges and Universities (HBCUs)
- 22% of the nation’s Hispanic Serving Institutions (HSIs)
SURA Programs

Jefferson Lab - DOE Office of Science - to probe nucleus of atom and study quark structure of matter

SCOOP - DOD Office of Naval Research/NOAA - to provide IT “glue” to integrate coastal research components

Information Technology - to build cyberinfrastructure foundation (the integration of high performance computing and networking) to support SURA’s scientific and research programs

Relations - to formulate and sustain internal and external relations strategy and support for SURA’s scientific and research programs
SURA Programs

**Jefferson Lab** - DOE Office of Science - to probe nucleus of atom and study quark structure of matter

**SCOOP** - DOD Office of Naval Research/NOAA - to provide IT “glue” to integrate coastal research components

**Information Technology** - to build cyberinfrastructure foundation (the integration of high performance computing and networking) to support SURA’s scientific and research programs

**Relations** - to formulate and sustain internal and external relations strategy and support for SURA’s scientific and research programs
Relevant History to Getting Here
(1 of 3)

- Began as university consortium to bid on, build and operate Thomas Jefferson National Accelerator, a.k.a. JLab
  - Still operating JLab today (www.jlab.org)
  - Collaboration among SURA members expanded as Internet came about
  - Built SURANet, one of the first regional networks connecting to NSFNet
Relevant History to Getting Here
(2 of 3)

- Formal IT Initiative formed in 2000, partially funded by SURANet proceeds
  - More formal & regular interaction with SURA CIOs
  - Initial focus on the physical network
  - Enterprise perspective moves “up the stack”
    - SURA partners with Internet2 and EDUCAUSE & manages NSF Middle Initiative Testbed, where enterprise & grid middleware meet
- SURA & participants’ involvement in NMI inspires SURAgrid project, www.suragrid.org
Relevant History to Getting Here
(3 of 3)

- SURAgrid perspective on authX is towards scalability of user and resource provider participation across administrative domains
  - Desire to leverage existing campus ID infrastructure, particularly PKI
  - Only as much centralized coordination as required to harmonize with campus infrastructure
  - SURAgrid Bridge CA as "interim" solution - but still in operation today
SURAggrid Access Management Model

SURAggrid Infrastructure:
Resources, Services, Communities, etc.

- Org CAs
- Campus CAs
- Dept. CA
- Users/Apps
- SURAggrid CA
- SURAgrid MS CA

Trust

Federation

Outside CyberInfrastructure

Non SURAggrid Campus/Regional Cyberinfrastructure

National Cyberinfrastructures

Corporate Resources
**SURAggrid Two-Tiered PKI - Anticipated Integration with Globally-focused Trust Mechanisms, Academic and Beyond**

**Higher Ed/Research Sector**
- Teragrid
- Other research grids, e.g. OSG
- HEBCA
- HE Campus Grids

**Non-research Federal Sector**
- FBCA
  - Federal Bridge Certificate Authority
  - R&D and informal collaborations

**Commercial Sector**
- Under investigation

**Member A’s SURAggrid Users**
- Member A’s Grid
- SURAggrid Member A’s CA
- Cross-certified pair
- SURAggrid CA (Not here yet...)
- SURAggrid CA (added Aug 08)
- Member B’s Grid

**Member B’s SURAggrid Users**
On SURA Focus at Fed/Ed 18

- Need to be ready for globally-oriented authX policies and technologies as they emerge
- Broader understanding of grids as a component of CI, and CI as next level research infrastructure
- Priority rising for larger set of SURA CIOs
  - *How can SURA best facilitate and support effective growth and use of CI in the region?*
10. Report on IDABC

eID interoperability: multi-level authentication and common specifications

John Stienen
European Commission, DG Informatics, IDABC Programme
12th TF-EMC2 Meeting, Utrecht, 4 December 2008

Manchester Ministerial Declaration

- No citizen left behind – inclusion by design
  - By 2010 all citizens become major beneficiaries
  - ICT for efficient and effective government
  - By 2010 high user satisfaction
  - ICT for efficient and effective government
  - Delivering high impact services
  - By 2010 100% e-procurement available, 50% take-up
  - By 2010 deliver other high impact services for growth and jobs
- Trusted access by means of eIDM across the EU
  - By 2010 interoperable eIDM for public services across the EU
  - By 2010 electronic document recognition framework

(24 November 2005)

i2010 Action Plan

- 2007: Agree common specifications for interoperable eIDM in the EU.
- 2008: Large scale pilots of interoperable eIDMs in cross-border services and implementing commonly agreed specifications.
- 2010: Review the uptake by the Member States of the European eIDM framework for interoperable eIDMs.
**Single Market Review**

A single market for 21st century Europe COM(2007) 724 final

- ICT is essential for the good functioning of the "e-Internal Market", creating interoperable services such as e-invoicing, e-procurement and e-customs. With the rapid development of these technologies, there is the risk that Member States opt for different or incompatible solutions, and that new "e-barriers" would emerge for the end users. The Member States and the Commission, working together, need to redouble their efforts to avoid market fragmentation and promote commonly agreed ICT solutions.

- Building on on-going work in the field of e-government, the Commission will present in 2008 a specific Action Plan to further promote the implementation of mutually recognised and interoperable electronic signatures and e-authentication (electronic identity) between the Member States, thereby facilitating the provision of cross-border public services.

---

**Security in Community legislation**

- **COM/2004/356**: allow secure and fast access to comparable public health data and to patient information.
- **COM/2005/608**: set up secure, integrated, interoperable and accessible electronic customs systems for the exchange of customs declarations, electronic certificates, accompanying documents and other information.
- **Council Directive 2006/112/EC**: Invoices sent or made available by electronic means shall be accepted (…). Provided that the authenticity of the origin and the integrity of their content are guaranteed (…) by means of an advanced electronic signature.
- **Directive 2006/123/EC**: … all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means...

---

**Action Plan e-signatures and e-identification**

- Based on the existing legal framework.
- **Horizontal actions** to improve cross-border use of online public services.
- Takes into account the work already done and currently ongoing (e.g., follow-up for IDABC studies on ID and eSignatures, feasibility study for Validation Service).
- Underlines importance of STORK and PEPPOL.
- Actions to improve transparency and trust; elaboration of guidelines.

---

**eSignatures study (2007)**

- Preliminary study on mutual recognition of eSignatures.
  - Studied a total of 127 eGovernment applications described in details in 29 country profiles (27 MS + 2 CC).
  - Analyses the requirements in terms of interoperability of electronic signatures for different eGovernment applications, and to provide recommendations on how to improve interoperability.
  - Provides an overview of applications per Member State concentrating on:
    - The type of electronic signature legally required.
    - The applicable technical restrictions.
  - Makes a proposal on how to disseminate the results, e.g. through a mutual information mechanism on electronic signature requirements.
**eSignatures study main conclusions**

- **Dissemination** of available information on national practices should be improved
- There is a link and sometimes **confusion** between the concepts and implementation of **authentication** and **electronic signatures**
- The trend is toward **PKI solutions**, hence this is where initiatives should focus
- A federated **validation solution** is needed to permit the validation and the establishment of trust for foreign signatures. Member States’ opinions on EU involvement and the role of the private sector should be sought

**eID Interoperability study (2007)**

A strategy for eID Interoperability that includes:

- A **survey and comparison** of the national eID legal instruments and national technical solutions implemented in 27+2+3 Countries
- A market assessment of the **ID Management technical solutions**; in particular a high-level description of the concept of federated identities
- A proposal and an impact assessment of a **multi-level authentication mechanism**
- **Common specifications** for interoperable eID solutions Based on existing actions at the EU level:
  - E.g. Modinis Study on ID Management in eGovernment, IST projects GUIDE, FIDIS and PRIME, work by the Porvoo Group, etc...

**eID Multilevel authentication mechanism**

- A multilevel authentication model that is universally applicable taking into account local preferences, sensitivities and existing infrastructure
- Technology neutral (i.e. **not exclusively PKI**)
- **Inclusive**, i.e. covering all possible registration mechanisms
- Covering at a minimum requirements for **risk management, registration** policies, and **authentication** as such
- Resulted in four **Authentication Assurance Levels**, in terms of risk and potential damage in case of abuse with registration requirements for solutions to be used and authentication requirements

  - ENISA’s work on **Authentication Interoperability**

**eID Draft Common Specifications**

- An overview of **requirements for a pan-European eIDM infrastructure**, covering legal, socio-cultural, technical, organisational aspects, while keeping in account local preferences, sensitivities and existing infrastructure
- Design principles:
  - federated, **multilevel**
  - relying on **authentic sources**;
  - allowing a context/sector based approach; and
  - enabling **private sector** uptake, as soon as appropriate

  - To be tested and developed further, e.g. in line with the STORK Pilot (WP5)

Competitiveness and Innovation framework Programme (CIP)

Ongoing work

- Qualified electronic signatures
  - 2009/Q3: update Decision 2003/511/EC
  - 2009/Q2: "Trusted List of Supervised Qualified Certification Service Providers" at European level.
  - 2009/Q3: guidelines on common requirements
- Advanced electronic signatures
  - 2009/Q2: eSignature study: updated country profiles
  - 2009/Q2: European federated validation service feasibility study
- eID
  - 2009/Q4: e-ID study: updated country profiles
  - 2008-2011: CIP ICT-PSP Pilot "STORK"
  - 2009: creation of a eID forum on epractice.eu

Trusted List of supervised (Q)CSPs

European Web site
Published List of supervised CSPs by country

Country Y

(cf. ETSI TS 102 231)

Country X

ICT Policy Support Programme Large Scale Pilots

- Competitiveness and Innovation framework Programme (CIP)
- Pilot’s areas defined by Member States in the context of agreed political declarations (e.g. Manchester declaration)
- eGovernment call 2007 → two Large Scale Pilots on Interoperability, with direct involvement and leadership of Member States:
  - EU-wide public eProcurement
  - Pan-European recognition of eIDs

Implementation of an integrated EU-wide electronic public procurement solution...

Implementation of an EU wide interoperable system for recognition of eID and authentication...

...enabling companies, in particular SMEs, from one state to respond to public procurements in any other state.

...enabling businesses, citizens to use their national electronic identities in any Member State

STORK

PEPPOL
STORK

- 14 countries, 29 consortium partners, public and private sector organisations
- AT BE DE EE ES FR IS IT LU NL PT SE SI UK
- 20 MC in 3 years, 50% co-funded by CIP
- Implements an EU wide interoperable system for recognition of eID and authentication and will:
  - Develop common rules and specifications to assist mutual recognition of eIDs across national borders
  - Test, in real life environments, secure and easy-to-use eID solutions for citizens and businesses
- Interact with other EU initiatives to maximise the usefulness of eID services.
  - WP2: “eID Inventory, Trust, and Application Groups”
  - WP5: “Common Specifications”

See [http://www.eid-stork.eu](http://www.eid-stork.eu)

More information

- The IDABC Programme: [http://ec.europa.eu/idabc](http://ec.europa.eu/idabc)
e-mail: idabc@ec.europa.eu