AGENDA

9:00am   Welcome and Introductions

9:15am   Drivers for EA2 from (one school’s) Applications Perspective
         Charlie Leonhardt, Principal Technologist, Georgetown University

9:45am – 10:15 am   The METEOR Network: An Early Success
         Tim Cameron, Meteor Project Manager, NCHELP

10:15am – 10:30am  Break

10:30am – 11:00am  Overview of InCommon Federation and Internet2 Middleware
         Ken Klingenstein, Director of Internet 2 Middleware Initiative, Internet2

11:00 a.m. - noon  Discussion on Barriers to Widespread Implementation of EA2
         Rob Abel, CEO, IMS Global Learning Consortium

noon – 1:00pm  Lunch

1:00pm – 2:00pm  Opportunities and Means to Overcome Barriers
         David Temoshok, Director of Identity Policy and Management, US GSA

2:00pm – 3:00pm  Next Steps: Work of the Task Force
         Discussion of Projects to Spur Adoption

3:00pm   Adjourn
Questions and Topics

Some questions to stimulate initial discussion to define strategy and scope of the Task Force, and to elicit suggestions and sources of information and data that would be useful to the Task Force.

1. What should be the basis for an investment in e-authentication and e-authorization in higher education—service to students, to faculty, or to employees, improved productivity, institutional reputation, improved security, or some combination?

2. How important should “Return on Investment” be compared to other motivations?

3. What have been successful data exchanges or projects that could contribute to successful data exchanges? What implementations or projects have failed to meet their expectations and may have lessons that would be useful to the community? (This could be the basis for case studies).

4. What are the barriers that prevent beneficial implementations of e-authentication or e-authorization?

5. Who are the suppliers to higher education? Which supply chains use electronic data exchanges? Which would benefit from EA2 implementation or from using different EA2 technologies?

6. What implementations would have high “Return on Investment” in higher education? How would prioritize those?

7. Which implementations are dependent upon changes in the “supply chain” itself? What are the barriers? What are the risks?

8. How does the community get the level of commitment among institutions needed for success? Are there examples? What prevents achieving that level of commitment?

9. What collaboration is needed across the standards-setting organizations to ensure the most effective implementation of EA2? How is this best achieved?

10. How do you balance scope of the standards with acceptance and willingness to implement? How do you resolve differences for areas within the scope of more than one standards-setting organization?

11. What are the motivations for software suppliers to cooperate? How can these be reinforced to encourage broader implementations?
Task Force Members

Charles Leonhardt, Principal Technologist, Georgetown University, Task Force Chair

Charles Leonhardt is Principal Technologist, Office of Information Services, Georgetown University. He is the primary advisor to the Vice President for Information Services and Chief Information Officer (CIO), and the University administration, on technology issues. He is responsible for the University's strategy for the development and enhancement of Scholarly Information Services that directly support pedagogical and research activities at Georgetown.


Charlie has an M.S. in Information Systems from American University and a Bachelor's in Economics and Philosophy from Georgetown (C'79).
Rob Abel, CEO, IMS Global Learning Consortium

Ellen Blackmun, Director of Technology Initiatives and Distance Learning, National Association of Student Financial Aid Administrators (NASFAA)

Tim Cameron, Project Manager, National Council of Higher Education Loan Programs (NCHELP)/Meteor

Tim Cameron is currently serving as the Project Manager for the National Council of Higher Education Loan Program’s (NCHELP) Meteor initiative. In this role, Tim is responsible for the project planning, oversight of all development tasks, production support service providers, communications and outreach for the project. Meteor is a web services tool that utilizes open source architecture to aggregate data from multiple sources nation wide for display in a single, aggregated view utilizing a federated model for authentication and authorization.

Tim has been involved in the higher education financing industry for nearly 18 years. He has worked for a loan servicer, a guarantor, and a national lender. Additionally, Tim has served as Chief of Staff for Financial Partners at the U.S. Department of Education and held the position of Vice President of Technology Services for NCHELP. His focus over the years has been in the electronic services area playing a primary role in both the development of and the implementation of industry standards.

Charlie Coleman, Director, CIO Application Development, Office of Federal Student Aid (FSA), U.S. Department of Education

Mr. Coleman currently serves as the Director, Application Development in the Office of Federal Student Aid / Department of Education. Previously, Charles was with ACTION and the U.S. General Accounting Office (GAO) where he was involved in various aspects of public administration and financial management. He also worked on Capitol Hill with the House Committee on Government Operations and the Senate Committee on Governmental Affairs.
Charles has served on other public sector committees, including the Council on Excellence in Government, and has been an active member of civic and volunteer organizations. He, his wife Beth, and daughter Lauren live in Lake Ridge, Virginia.

**Larry Fruth**, Executive Director, Schools Interoperability Framework Association (SIFA)

**Ken Klingenstein**, Director of Internet 2 Middleware Initiative, Internet2/InCommon

Dr. Ken Klingenstein is Director of the Internet2 Middleware and Security areas and Chief Technologist at the University of Colorado at Boulder. In his Internet2 middleware role, he is responsible for fostering the development and dissemination of middleware interoperability and best practices, through partnership efforts of leaders among campus IT architects, corporations, and government agencies. In his Internet2 security role, Klingenstein is helping campus network security leadership to develop approaches to both immediate issues such as network authentication and new security tools, as well as developing longer-term agendas that couple increased security with research network goals of performance and transparency. As Chief Technologist for the University of Colorado Boulder campus, he continues to provide technical strategic leadership for information technology for the institution where he served as Director of Information Technology Service for fourteen years. Klingenstein has been active in national and regional networking for many years, serving in leadership positions in too many organizations. Dr. Klingenstein received his Ph.D. in Applied Math from the University of California at Berkeley.

**Nancy Krogh**, Registrar, University of Idaho, American Association of Collegiate Registrars and Admission Officers (AACRAO)
Hans L’Orange, Director, SHEEO/NCES Network and Director of Data and Information Management, State Higher Education Executive Officers (SHEEO)

Hans P. L’Orange is Director of Data and Information Management and Director of the SHEEO/NCES Network for the State Higher Education Executive Officers (SHEEO). SHEEO was created in 1954 as a membership association to help its members and the states develop and sustain excellent systems of higher education. The boards served by the members of SHEEO are responsible for advising governors and legislatures on policies to strengthen higher education's contributions to the states and for performing the governance and coordinating functions assigned to them by law. The Network is a collaborative project administered by SHEEO and funded by the National Center for Education Statistics (NCES) at the U.S. Department of Education.

Mr. L’Orange serves as a liaison to foster communication, cooperation, and collaboration between the federal government, state higher education agencies, and national associations on issues related to data collection, data management, and information dissemination. His primary areas of interest and responsibility are developing effective strategies for data management; the relationships between data, information, and knowledge; and using knowledge resources effectively to impact public postsecondary education policy.

Director of the Network since 1998, Mr. L’Orange was previously the Associate Director for Institutional Analysis at the University of Colorado at Boulder. He received his M.S. degree in business information systems with a minor in organizational development from the University of Colorado and a B.A. degree from Colorado State University.

Adele Marsh, Vice President of Industry Initiatives, AES, representing the PESC Standards Forum for Education

Adele Marsh is Vice President for Industry Initiatives at American Education Services (AES). With over thirty years of experience in the financial aid industry, Adele has been an active participant in various
efforts to advance industry standards and practices. Her extensive financial aid experience has made her a valued contributor to many programs which have helped shape the future direction of the industry.

Adele is currently providing leadership to several key initiatives. She is the Chair of the PESC Standards Forum Steering Committee, Co-Chair of the Meteor Advisory Team, and Team Leader for Mapping Your Future Technology/Data Exchange.

Adele started her career in the Financial Aid Office at Millersville University of Pennsylvania before joining AES.

**Brett McDowell**, *Executive Director, Liberty Alliance*

**David Temoshok**, *Director of Identity Policy and Management, U.S. General Services Administration, Electronic Authentication Partnership (EAP)*

**Steve Worona**, *Director of Policy and Networking Programs, EDUCAUSE*
# EA2 Task Force

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Organization/Association</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jill Abbott</td>
<td>SIFA Learning Strategist</td>
<td>Schools Interoperability Framework Association (SIFA)</td>
</tr>
<tr>
<td>Rob Abel</td>
<td>CEO</td>
<td>IMS Global Learning Consortium</td>
</tr>
<tr>
<td>Ellen Blackmun</td>
<td>Director of Technology Initiatives and Distance Learning</td>
<td>National Association of Student Financial Aid Administrators (NASFAA)</td>
</tr>
<tr>
<td>Charlie Coleman</td>
<td>Director, CIO Application Development</td>
<td>Office of Federal Student Aid (FSA) U. S. Department of Education</td>
</tr>
<tr>
<td>Ken Klingenstein</td>
<td>Director of Internet 2 Middleware Initiative</td>
<td>Internet2/InCommon</td>
</tr>
<tr>
<td>Nancy Krogh</td>
<td>Registrar</td>
<td>University of Idaho representing American Association of Collegiate Registrars and Admission Officers (AACRAO)</td>
</tr>
<tr>
<td>Mark Luker</td>
<td>Vice President</td>
<td>Educause</td>
</tr>
<tr>
<td>Charles Leonhardt</td>
<td>Principal Technologist</td>
<td>Georgetown University representing Postsecondary Electronic Standards Council (PESC)</td>
</tr>
<tr>
<td></td>
<td>Task Force Chair</td>
<td></td>
</tr>
<tr>
<td>Hans L'Orange</td>
<td>Director, SHEEO/NCES Network and Director of Data and Information Management</td>
<td>State Higher Education Executive Officers (SHEEO)</td>
</tr>
<tr>
<td>Adele Marsh</td>
<td>Vice President of Industry Initiatives</td>
<td>AES</td>
</tr>
</tbody>
</table>

One Dupont Circle NW ~ Suite 520 ~ Washington, D.C. 20036
202-293-7383
www.PESC.org
<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georgia Marsh</td>
<td>Deputy Director, Federal E-Authentication Initiative</td>
<td>U.S. General Services Administration</td>
</tr>
<tr>
<td>Brett McDowell</td>
<td>Executive Director</td>
<td>Liberty Alliance</td>
</tr>
<tr>
<td>David Temoshok</td>
<td>Director of Identity Policy and Management</td>
<td>U.S. General Services Administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electronic Authentication Partnership (EAP)</td>
</tr>
</tbody>
</table>

**Attendees**

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jon Allen</td>
<td>Media Producer</td>
<td>instructional media + magic, inc.</td>
</tr>
<tr>
<td>Joshua Aversa</td>
<td>Product Manager</td>
<td>SunGard Higher Education</td>
</tr>
<tr>
<td>Thomas E. Board</td>
<td>Director, IT Systems Architecture</td>
<td>Northwestern University</td>
</tr>
<tr>
<td>Mark Bolesbach</td>
<td>Principal Analyst</td>
<td>SunGard Higher Education</td>
</tr>
<tr>
<td>Barbara Clements</td>
<td>Chief Standards Officer</td>
<td>National Transcript Center</td>
</tr>
<tr>
<td>Jim Farmer</td>
<td>Chairman</td>
<td>instructional media + magic, inc.</td>
</tr>
<tr>
<td>Susan McCrackin</td>
<td>Director, Financial Aid Services</td>
<td>The College Board</td>
</tr>
<tr>
<td>Scott A. Rea</td>
<td>Director, HEBCA OA – ISTS</td>
<td>Dartmouth College</td>
</tr>
<tr>
<td>Neil Sattler</td>
<td>Program Specialist</td>
<td>Office of Federal Student Aid (FSA)</td>
</tr>
<tr>
<td>Name</td>
<td>Position</td>
<td>Institution</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Michael Sessa</td>
<td>Executive Director</td>
<td>U. S. Department of Education</td>
</tr>
<tr>
<td>Rick Skeel</td>
<td>Director of Academic Records</td>
<td>University of Oklahoma</td>
</tr>
</tbody>
</table>
Task Force Chair Charlie Leonhardt opened the meeting by giving “One School’s View.” As he experiences what schools, faculty, students and alumni want from information technology, the answer is “everything, now, anywhere.” The Task Force should focus on institutionally delivered products and services. “Identify management is a driver.”

The online systems used for teaching and learning—scholarly systems—are still immature, but will later manage learning. They will be mission critical and most sensitive to security.

The Meteor Project

Adele Marsh briefed the Task Force on the Meteor Project. Financial aid administrators and now students may, through any “access provider,” receive reports on student loans consolidated in real time from data available at “data providers” via an “index provider”—the National Student Clearinghouse—that has data on sources of information. This is done using cryptographically encoded XML SOAP messaging.

She said the application is consistent with federal and state laws on privacy. There is an algorithm to ensure the display reduces ambiguity of data from multiple sources. The application has a “Level of Assurance” associated with the user identity consistent with the federal government’s definition. The Meteor software is provided based on a signed agreement from the college or university about security. Meteor does not audit security.

Internet 2/InCommon

Ken Klingenstein briefed the Task Force on InCommon. The InCommon Federation creates and supports a common framework for trustworthy shared management of access to online resources in support of education and research in the United States. InCommon is facilitating development of a “community-based common trust fabric sufficient to enable participants to make appropriate decisions about access control information provided to them by other participants.” InCommon uses Shibboleth® as its federating software.

Ken cited ProtectNet as an independent Identity Provider (IdP) supporting Shibboleth for several organizations.

He reported that Shibboleth 2.0 Alpha is scheduled for April 2007. (Meteor would like to use/needs version 2.0).
Barriers to Widespread Implementation of EA2 – Rob Abel, IMS Global Learning Consortium

Rob Abel commented that barriers depend upon the application. He would prefer to focus on “opportunities for federation” and applications worthy of “mass implementation.” He commented higher education is “in transition” to integrated online applications within and across institutions. He commented that cross-over of information from high school to college is difficult. Perhaps escalating the Level of Assurance issue would be helpful.

Scott A. Rea, Director, Higher Education Bridge Certificate Authority, Operating Authority, Dartmouth College, commented “opportunities” should be based on the driving forces for federation.

Ken commented when a federation moves from ad hoc to production is when the policy issues must be fully resolved. He said streaming media is an application in higher education that requires authentication and authorization. He said most use the eduPerson equivalent for authentication. InCommon uses an LOA (Level of Assurance) paradigm.

Jill Abbott, Schools Interoperability Framework Association, said that SIFA has data models for exchanges that are widely implemented.

Adele said “identify proofing” is key to trust.

Hans L’Orange, Director SHEEO/NCES Network, State Higher Education Executive officers, echoed that K-16 alignment is important and there should be backward linking from higher education to K-12.

Ken Klingenstein pointed out the Level of Assurance changes with additional experience with and information about the user.

Rick Skeel said eAuthentication/eAuthorization should be based on “needs of the student.” He also commented registers never see some students, especially in distance learning. Higher education may need to rely on earlier relationships.

Barbara Clements said there is needed for identifying parents and the definition of patent for different purposes. She also said there are many high school students who are taking college courses while in high school. And also that teachers are often students at the same time.

Ken said you can begin identification using only a gmail or Hotmail account. This is the beginning of the process.

One of the attributes now requested by relying parties is for “green card status.” [As an example of need driving requirements for collecting and maintaining attributes].
Brett McDowell, Executive Director, Liberty Alliance, commented that trust [and the need for attributes] depends upon jurisdiction. Federations will be international; the European Union is an example of emerging federations.

Ken commented that illegal immigrants is becoming a higher education concern. He asked “What attributes are required for proof of citizenship? This is state specific.”

Hans said the policy [or practice] is “trust but verify.”

Ron Abel summarized by saying application use cases define the criteria for authentication and authorization. He saw an opportunity to document and recommend attributes.

Hans said it is important this be done in an operational context.

Rob said the Task Force should look to the “value to the student.” And consider the full “lifecycle of the student.”

Mark Luker, Vice President, Educause, said the Task Force should look for opportunities to “save money”—savings are a driver for implementation.

Brett commented the value proposition is better for the student and if the student receives value, perhaps the student should pay.

Adele said in Meteor students and schools never pay; the service is provided at no cost. The application does benefit the lenders [providing financial support and staff time to the project].

Rob said perhaps where a scenario showed most valuable to the student, then charge a premium to the student.

Charlie Coleman, Director, CIO Application Development, U.S. Department of Education, said FSA is starting in a small way with institutions—which includes 6,500 colleges and universities. All have institutional reports.

Charlie Leonhardt asked if the Department of education’s model could be used for higher education. Is there unwillingness by anyone to participate? What do we find in the government sector? Perhaps regional models with a “best on win” practice is reasonable.

Brett asked what federations exist [in higher education].

Adele comment with SAML2.0 federation is feasible [that is, now supported by SAML].

Brett commented that policy should begin first, and then consider technology.
Rob Abel asked if there was a federation of the University of California system with high schools for apply [to the university] or for graduate applications.

Ken said federation follows political structures.

Brett said the European Union took three years for four federations. Those doing federation have a “branding” advantage.

Rob commented the “branding” is advantageous with articulation.

Rick Keel said there were increasing dual enrollments, research across organizations, and library [that would benefit from federated authentication/authorization].

Hans said portfolios—“collection of items”—is an example where authentication/authorization is required. Common application [for admissions] is another application.

Adele commented that institutions benefit.

Jill said there are savings in administration.

Ken commented authorization is a “big space.” Roles are needed. Normalization of one or two roles would be helpful. This should be done consistent with external standards.

Barbara said access may require an “education purpose”—which is a role issue.

Ken said no one attribute or combination is normative.

Hans said institutional research has a limitation.

Rob summarized saying the focus should be on simultaneous access scenarios. Understand the policy issues. Find the business drivers.

Scott commented that institutions provide additional services.

Rob said membership in a federation is “branding.”

Barbara said most K-12 access is through state portals.

Jill said this varies state to state.

Ken said partnerships are important and lad to federated identify and federations.

Scott summarizing saying federateable eAuthentication/eAuthorization 1. Makes the job easier, 2. benefits students, 3. ensures compliance, and 4. “looks good.”
Ken said disability object classes is another candidate for standardization. Dave Temoshok said the more precise term is “508 compliant.”

Ken also commented that pictures may be required for authentication.

Rob said learner preferences is another application since they could span applications.

Ken asked who is the authority for attributes for “08 compliance.”

Opportunities and Means to Overcome Barriers – David Temoshok, Director identity Policy and Management, U.S. General Services Administration

In his opening comments, David said without a national ID, the federal government will have to rely (trust) non-federal identity providers. The federal government will follow NIST (National Institute of Standards and Technology) standards for Level of Assurance. EAP (Electronic Authentication Partnership) has adopted the federal standards.

The federal government not only made the work they’ve completed openly available, but also certified [initial] credential service providers. GSA would like fo the certification of credential service providers to be done external as well. EAP is working on certifying credential service providers.

There are three challenges for identity federation to be successful:

- Learn how to trust another entity
- Work across organizations (via a means such as SAML 2.0 and/or X509)
- Needs a “network” administration—someone who makes sure that the rules are followed. A way to manage relationships.

Most develop a common set of tules for trust, interoperability and business.

Would need additional agreements for authorization. Three universities attempted to be certificated, but abandoned the effort when documentation of their practices and software did not meet the criteria. Federal guidelines are needed for a federation operator.

The federal government established governance structures. The Governance structure must determine how rules are established and enforced.


Scott said often authorization is based on role rather than identity.
David said “David’s Plan”—not yet a government plan—would be to have an independent auditor and industry providers.

Ken said there need to be federal guidelines and possibly a federal operator when there is inter-federation needs for authentication or authorization.

David described the federal implementation. Ken confirmed that none of the universities anticipating exchange with federal agencies passed the evaluation. These universities were seeking certification for Level of Assurance 1 and 2.

Scott said the biggest barrier is liability. This requires time and patience.

Brett said you have to build trust and resolve the liability issue.

Charlie Leonhardt said one alternative is to encourage the participation in InCommon. And other is to find a “killer application” important to both the colleges and universities and the vendor community.

David said Educause and the bridge [between federal and higher education] was a project that had been technically successful.

Charlie Leonhardt said it would be helpful if there was a federal project with a “carrot” for the colleges and universities.

Brett said there were three steps; 1. Technology for interoperability and inter-federation exchanges, 2. Policies supporting operation and 3. Certification of federation members.

An observation that the NSF FastLane project “plug was pulled because of lack of trust between federations—Federal and Incommon.

What Next – Charlie Leonhardt

Need to develop use cases, preferably 3 to 5 “killer applications.”

“One pager” to introduce the project to members and participating organizations.

Task Force would use:

1. E-mail and conference calls

2. Later decide when to meet in person (Michael Sessa suggested at the Montreal PESC meeting for one of these meetings).

3. Listserv should be set up for the Task Force
Task Force Members in Attendance:
- Jill Abbott (Schools Interoperability Framework)
- Rob Abel (IMS Global Learning Consortium)
- Ellen Blackmun (NASFAA)
- Charlie Coleman (Office of Federal Student Aid, U S Department of Education)
- Ken Klingenstein (Internet2/InCommon)
- Nancy Krogh (University of Idaho representing American Association of Collegiate Registrars and Admission Officers)
- Mark Luker (Educause)
- Charles Leonhardt – Task Force Chair (Georgetown University representing Postsecondary Electronic Standards Council)
- Hans L’Orange (State Higher Education Executive Officers)
- Adele Marsh (AES representing PESC Standards Forum for Education)
- Georgia Marsh (U S General Services Administration)
- Brett McDowell (Liberty Alliance)
- David Temoshok (U S GSA representing Electronic Authentication Partnership)

Attendees:
- Joshua Aversa (SunGard Higher Education)
- Mark Boelmbach (SunGard Higher Education)
- Barbara Clements (National Transcript Center)
- Susan McCrackin (The College Board)
- Scott Rea (Dartmouth College)
- Neil Sattler (Office of Federal Student Aid, U S Department of Education)
- Rick Skeel (University of Oklahoma)

One School’s View – Charlie Leonhardt
- What do schools, faculty, students, alumni want? Everything, now, anywhere, etc.
- We should focus on institutionally delivered products and solutions.
- Identify management is a driver. Who gets ID card, who gets to authorize transcript, etc.
- Online systems that are directly used in teaching and learning – scholarly systems – still immature – isn’t really managing learning yet. Mostly course content management.
Meteor Presentation – Adele Marsh (See presentation)

Internet 2/InCommon – Ken Klingenstein (See presentation)
- Shib protected wikis - Spaces.internet2.edu Look at ProtectNetwork
- Shib 2.0 Alpha scheduled for April 2007.

Barriers to Widespread Implementation of EA2 Discussion – Rob Abel
- What scope are we really talking about? What are the driving forces for federating? Need carrots!! Is K-12 in our out of scope? Probably not where appropriate. Cross over from high school to college is difficult. Escalating Level of Assurance issue.
- AGREEMENT: Value to student is important and establishing identify as early as possible.
- Where is FSA on federated trust model? Starting small with schools, lenders, guarantors. E-campus based.
- BARRIER: Lack of long-term goals (leadership) from the Department of Education.
- UC system: Which would be better? Federating with high schools or the graduate admission scenario.
- Branding issues. Strategically, who gets to authenticate and who just receives the authentication?
- Student continues activity with one institution, but also has activity with another institution. How we handle that transition/transfer may be a better opportunity. Student’s educational capital moves to their control. Branding shifts. Also, relates to high school student taking college courses.
- Roles – identify a couple that we could focus on for authorization. Is there something out there that we should be looking at for role based access control.
- How to proceed: Simultaneous access scenarios – need to understand policy issues. Also, look at business drivers. Ability to offer additional services.

Opportunities and Means to Overcome Barriers – David Temoshok
- Without a national ID, the federal government will have to rely (trust) on non-federal identify providers.
- The federal government will follow NIST standards for Level of Assurance. EAP also adopted.
- The federal government not only made the work they’ve completed openly available, but also certified credential service providers.
- EAP is working on certifying credential service provers.
- Three challenges for identify federation to be successful:
  - how to trust another entity
  - must work across organizations (a means to communicate – SAML 2.0 and/or x509)
needs to be a “network” administrator – somebody who makes sure that the rules are followed – a way to manage relationships.

- Must develop a common set of rules. Trust, interoperability, business rules.

- May also need some additional items for authorization. Three campuses have attempted to be certified, but documentation did not meet the criteria. What about the rest of higher ed? Assessment needs to be done with integrity and should probably be done by an independent body (for example, a SAS70 audit). Or a third-party organization such as the EAP. Federal guidelines are needed for a federation operator.

- The federal government established governance structures. Governance structure must determine how rules are established and enforced. The federal government is looking at how to recognize non-federal federations. Looking to rely on the administrative policies and procedures of some other entity.

- Common software (Meteor) vs. independently developed software that speaks SAML (identity management software) – then have to make sure that those products work with what you’ll be communicating.

Opportunities Discussion – All

- Potential Projects:
  - InCommon and Federal Government federation trusting each other. How does that happen and when? Today – must join federal government federation and must be certified by GSA.
  - Work with Educause to recognize a higher education bridge or InCommon to support the same constructs. Three layers – technological interoperability, operational trust, and certification.
  - Talk to the Department of Education to find some carrots.
  - Meteor and InCommon interoperability.
  - Need to educate the legal community.
  - Higher education has many levels of complexity.

- NSF FastLane project – plug was pulled because of lack of trust between federations. (Federal federation and InCommon).

- Need to develop use cases.
  - 3-5 Killer apps.

- One pager to introduce to members or participating organizations.

- How should we operate?
  - E-mail and conference calls.
  - Once we map things out, we will determine when to meet in person.
  - Listserv will be set up.
Attachments:

Meteor Presentation

Internet2/InCommon Presentation
What is Meteor?
- Web-based universal access channel for real-time inquiry of financial aid information
- Aggregated information to assist Financial Aid Professionals, students and borrowers with debt counseling and the aid process in general
- Collaborative effort of leading FFELP providers
- Freely available software and access to the network

The Meteor Project Components
- The Meteor Software
- The Meteor Network
- The Meteor Federation

Meteor Software Features
- Information from multiple data providers is aggregated in real-time to assist the FAP and the borrower with the financial aid process, repayment and default aversion.
- Meteor is a collaborative effort utilizing leading-edge technology and access is provided at no charge.

Types of Data Available
- FFELP
- Alternative/Private Loans
- State Grants & Scholarships (Planned)
- Perkins (In development)
- Direct Loans (Planned)
- Pell Grants (Planned)

Meteor Software Features
- Access timely, student-specific financial aid information from multiple sources
- One-stop, common, online customer service resource
The Meteor Network

- Meteor
  - Federated Model: Transitive Trust
  - Multiple points of access
- User Roles
  - School
  - Student/Borrower
  - Customer Service Representatives
  - Lenders

Use of data approved by FSA

- FSA approval for use of real-time data
  - Collaborative effort to bring about change to the requirements for schools to solely rely on NSLDS
  - Allows schools to resolve discrepancies by using real time data that comes directly from the loan holders' databases

The Meteor Process

- Federated model of authentication
- Meteor Participant Certification
- Conditions of Use
- Authentication protocol review
- Use of Data Exception Policy

Building Trust and Integrity

- The Meteor Advisory Team sought input and expertise regarding privacy and security from the sponsoring organizations and the NCHELP Legal Committee.
- Analysis was provided in relation to Gramm-Leach-Bliley Act (GLBA), and individual state privacy laws.
- The analysis revealed that Meteor complied with both GLB and known state privacy provisions.

E-Authentication

- The MAT worked with the Shibboleth project, a project of Internet2/Mace, in developing architectures, policy structures, practical technologies, and an open source implementation to support inter-agency sharing of web resources.
- Shibboleth project participants include Brown University, Ohio State, Penn State and many other colleges and universities.
Reliability and Security

- Data is sent directly from the data provider’s system and is not altered in any way within Meteor.
- All data is electronically transmitted securely using SSL encryption.
- Independent Audit showed no serious vulnerabilities.

Meteor’s Authentication Objectives

- Provide a flexible, easy to implement authentication system that meets the needs of the provider organizations and their customers.
- Ensure compliance with the Gramm-Leach-Bliley Act (GLBA), federal guidelines, and applicable state privacy laws.

Meteor’s Authentication Objectives

- Assure data owners that only appropriately authenticated end users have access to data.
- Ensure compliance to participant organizations internal security and privacy guidelines.

Authentication

- No central authentication process
- Utilizes transitive trust model
- Each Access Provider uses their existing authentication model (single sign-on)
- Level of trust assigned at registration

The Meteor Authentication Model

- Each Access Provider uses their existing authentication model (single sign-on)
- Meteor levels of assurance are assigned at registration
  - Level 0 (Unique ID)
  - Level 1 (Unique ID & 1 piece of validated public data)
  - Level 2 (Unique ID & 2 pieces of validated public data)
  - Level 3 (Unique/User ID & shared secret)
- Meteor Level 3 complies with the NIST Level 2

Meteor’s Authentication Requirements

- User is required to provide an ID and a shared secret.
- Assignment and delivery of shared secret must be secure.
- Assignment of shared secret is based on validated information.
- Reasonable assurances that the storage of the IDs and shared secrets are secure.
E-Authentication Policies
- Access provider must ensure appropriate authentication for each end user and provide traceability back to that user.
- Access provider must provide authentication policy to central authority.
- Access provider must provide central authority with 30 day advance notice of changes to authentication policy.
- Access provider must agree to appropriate use of data.

The Meteor Authentication Process
- End user authenticates at access provider site or through a Meteor approved third party Authentication Agent.
- Access provider creates authentication assertion (SAML).
- Access provider signs authentication assertion with digital certificate.
- Control is passed to Meteor software.

The Meteor Authentication Process
- Index and data providers verify assertion using the access provider’s public key stored in the registry.
- End user is provided access to the aggregated data.

SAML Assertion Attributes
- Role of end user.
- Social Security Number.
- Authentication Process ID.
- Level of Assurance.
- Opaque ID.
- School OPEID (Summer 2007).

Current Status
- 1 Index Provider.
- 20 Data Providers.
- 15 Access Providers.
- 1 Authentication Agent.

Meteor Usage
- Meteor Usage:
  - FAA Statistics
  - Usage has been increasing since FSA announcement about use of real time data.
  - Borrower Statistics.
  - Meteor…not just an inquiry network.
  - In addition to providing access to and aggregation of financial aid award information, the Meteor software can also be used by organizations to enhance their current services.
    - MYF integration.
    - Internal usage of the software at member organizations.
Authentication and Authorization

- Authentication is the process of determining the identity of a user that is attempting to access a system.
- Authorization is the process of determining what types of activities are permitted.

Once you have authenticated a user, they may be authorized different types of access or activity.

- Meteor Roles
  - Financial Aid Professional
  - Student/Borrower
  - Customer Service
  - Lender

Authentication Process:

- Student logs into Access Provider site (i.e. school, lender, servicer or guarantor)
  - Access Provider authenticates student
  - Access Provider messages the Meteor Registry for validation, attaching the security assertion
  - Registry validates the provider and sends the request to the Meteor Index for processing.
  - The index identifies potential data providers who receive a message including the security assertion
  - Data providers return data to the access provider provided that the applicable authentication level meets their requirements.

What’s Next?

- Continue to monitor the development of XML, transport and authentication standards
- Review of multi-layer authentication
- Clock synchronization across the network for timing out of assertions for additional security
- Alignment with the NIST levels of assurance

Contact Information

Tim Cameron
Meteor Project Manager
NCHelp
703-960-8665
meteor@nchelp.org
InCommon, other federations, the attribute ecosystem, and some killer apps needing guns...

**Publisher’s Note**

The author of this presentation warns us "that the shelf life of the content has expired…. the problem with a rapidly moving area."

**Topics**

- International Federations
- State system federations, medical federations, and others
- InCommon
- Peering, confederation, nested and other relationships
- The rest of the attribute economy
- Some killer apps
  - Grad student admissions
  - Authenticated letters of recommendation

**International Federations**

- Widespread in Europe (over 15 countries), emergent in Australia, nascent in Asia.
- The UK federation (http://www.ukfederation.org.uk/) already has over five million active users and intends to grow to all of higher ed, K-12 and further education.
- Used for academic content access, research support, national level services, etc
- Clear needs for peering; some need for confederation or dynamic relationships.

**Public sector federations**

- State-based among health agencies (NY), presenting a SSO to citizens (Washington), etc.
- GSA EAuthentication
- State university federations - Texas, California, Maryland, etc
- InCommon

**InCommon**

- US R&E Federation
- www.incommon.org
- Members join a 501(c)3
- Addresses legal, LOA, shared attributes, business proposition, etc issues
- Approximately 50 members and growing
- A low percentage of national Shib use…
InCommon Members 2/27/07
- Case Western Reserve University
- Clemson University
- Cornell University
- Dartmouth
- Duke University
- Florida State University
- Georgetown University
- Miami University
- New York University
- Ohio University
- Penn State
- Stanford University
- Stony Brook University
- SUNY Buffalo
- The Ohio State University
- The University of Chicago
- University of Alabama at Birmingham
- University of California, Irvine
- University of California, Los Angeles
- University of California, Merced
- University of California, Office of the President
- University of California, Riverside
- University of California, San Diego
- University of Maryland
- University of Maryland - Baltimore County
- University of Maryland, Baltimore
- University of Rochester
- University of Southern California
- University of Virginia
- University of Washington
- University of Wisconsin - Madison
- Cdigix
- EBSCO Publishing
- Elsevier ScienceDirect
- Houston Academy of Medicine - Texas Medical Center Library
- Internet2
- JSTOR
- Napster, LLC
- OCLC
- OhioLink - The Ohio Library & Information Network
- ProtectNetwork
- Symplicity Corporation
- Thomson Learning, Inc.
- Turnitin
- WebAssign

Key aspects of InCommon
- Federating software
  - Shib 1.2+ (other possibilities in the future)
- Shared attributes and schema
  - eduPerson right now
- Levels of authentication
  - POP (participant operational practices)
  - InCommon Bronze and Silver will map to LOA 1 & 2
- Management
  - Steering committee of members IT executives
  - Operations staffed by Internet2

Shibboleth
- Shib 1.3 widely deployed; 1.2 still common
- Along the way, other capabilities added:
  - ADFS compatibility for WS-Fed, (MS $)
  - Eauthentification certification (with waiver form:)
- Shib 2.0 completes the SAML+Shib integration
  - More compatible with COTS SAML 2.0 products than they are with each other
  - A Shib/SAML to TCP/IP analogy isn’t bad; Shib adds multi-party federation support through metadata, ARPS, etc.
- Also eases support for n-tier, non-web and other capabilities
- Alpha in April

The Shibboleth 2.0 Sidebar
- Support for the attribute ecosystem
  - attribute handling, including policy, in both SP and IdP
  - designed to be reusable for other protocols (eg CardSpace)
- All Java SP (in addition to current Java/Apache), easing integration for some applications
- Trust management
  - PKI still seems too hard, even at the simpler enterprise level
  - Supports a broad set of trust choices – CA’s, certs, plain keys, managing site metadata (naming, acquisition, validating)
- A product of years of painful experience ☺

InCommon Management/Governance
- Steering Committee of campus/vendor CIO’s and policy people – sets policies for membership, business model, etc.
- Technical advisory committee - Sets common member standards for attributes (eduPerson 2.0), identity management good practices, etc.

InCommon Uses
- Access control to content
  - Popular content – Ruckus, CDigix, etc
  - Scholarly content – Google, OCLC WorldCat
- Downloads – Microsoft
- Access to external services
  - Student travel, charitable giving, web learning and testing, plagiarism testing service, etc.
  - Allure for alumni services and other internal businesses
  - Student loans, student testing, graduate school admissions, etc.
- Access to national services
  - The National Science Digital Library
  - The Teragrid pilot
Challenges in the US

- Addressing the risks in federated identity
- Too many lawyers
- Too few business drivers
  - No bulk content licensing
  - Few “national” applications
  - No government access yet
- Number of “big dog” institutions
- For many institutions, the focus is in state versus national for applications
- Bi-lateral relationships exist more than national relationships
- Single-purpose federations can leverage existing contracts.
- Not all institutions really have their identity management technologies fully in place
- Very few have their identity management policies in place.

Inter-federation key issues

- Peering, peering, peering
  - At what size of the globe?
  - Confederation
    - Tightly coupled autonomous federations
    - How do vertical sectors relate? How to relate to a government federation?
  - On what policy issues to peer and how?
    - Legal framework
      - Treaties? Indemnification? Adjudication
    - How to technically implement
      - Wide variety of scale issues
  - WAYF functionality
  - Virtual organization support

Peering

Possible peering parameters

- LOA
- Attribute mapping
- Economics
- Liability
- Privacy

VOs plumbed to federations

The Attribute Ecosystem

- We now understand, we think, an overall “attribute ecosystem”
- Shibboleth is the real-time transport of attributes from an IdP to an SP for an authorization decision
- Other, “compile-time” means are used to ship attributes from sources of authority to IdP
- Or to the SP, or to the various middlemen (portals, proxies, etc.)
- And a user needs to be manage all of this
User Application access controls (including network devices)

Shib

IdP

p2p

User Application access controls (including network devices)

Shib

IdP

p2p

A Simple Life GUI

A Full IdM Life

Application access controls (including network devices)

Shib

IdP

Local apps

User

p2p

A Full Life GUI

Application access controls (including network devices)

Shib

IdP

Local apps

User

p2p

Source of Authority

Source of Authority

Source of Authority

Relative Roles of Signet & Grouper

RBAC (role-based access control) model

• Users are placed into groups (aka "roles")
• Privileges are assigned to groups
• Groups can be arranged into hierarchies to effectively bestow privileges
• Grouper manages, well, groups
• Signet manages privileges
• Separates responsibilities for groups & privileges

A Full Life GUI

Application access controls (including network devices)

Shib

IdP

Local apps

User

p2p

Signet/Grouper

Source of Authority

Source of Authority

Source of Authority

Real Life

Application access controls (including network devices)

Shib

IdP

User

p2p
**Killer Apps**

- Graduate school admissions
  - Group, including UW, Cornell, and UWisc, starting conversations on “student process improvement via authn/federation”
  - Current approaches to letters of reference has significant exposure
  - Student viewing of grad application status is classic “yet another account/password”
  - Federal apps, from Fastlane to NIH to the Dept of Ed

- **Opportunities for action**
  - The application of federated identity to improve student processing, etc…
  - Beginning to wade upstream within institutional SOA to distill good practices

**Killer Apps**

- Outsourced services
  - Scholarly services - TurnItIn, WebAssign
    - Trust model for SPEEDE?
  - Benefits
  - Dorm room matching, travel
  - Alumni
- Professional societies for their peer review, content access, etc.
FOR IMMEDIATE RELEASE
February 6, 2007
Contact: Michael Sessa
PESC Executive Director
202-293-7383

Inter-O rganizational Task Force to Advance Electronic Authentication and Authorization for Higher Education

Washington, D.C. ~ The Board of Directors of the Postsecondary Electronic Standards Council (PESC) is pleased to announce the launch of an inter-organizational eAuthentication/eAuthorization (EA2) Task Force. Representatives from eleven associations and from the U.S. Department of Education, who will serve as Task Force Members, will plan and seek implementation of common eAuthentication/eAuthorization technologies and practices to enable trusted exchange of data among colleges and universities and the federal and state government departments and agencies, and suppliers. Based on widely used open standards, a decade of development, and the successful experience of several projects, the EA2 Task Force expects the results of their work to sharply improve service to students, faculty, and the public; and, to improve security and lower unit costs.

Task Force Chair Charles Leonhardt, Principal Technologist at Georgetown University, states, “The first charge is identifying barriers to broad implementation of the availability technologies and standards. Then we can prioritize the tasks to make most use of current technology and available resources.”

Rob Abel, CEO of IMS Global Learning Consortium, adds, “More and more colleges and universities are using IMS specifications for exchanging learning services and for enterprise integration. We are pleased these will be part of a broad implementation initiative.”

PESC’s Executive Director Michael Sessa states, “Projects currently in production — NCHELP’s widely implemented Meteor Network, PESC’s suite of electronic XML transcripts, JSTOR’s Shibboleth implementation in the U.K. for electronic journals, and CRC’s broadening implementation in financial aid for examples — have demonstrated feasibility, reliability, and security of electronic data transfer. These experiences can be the basis for large-scale implementations.”

“eLearning is being implemented widely to improve our teaching and learning.” Mr. Leonhardt continues. “Now we are integrating eLearning with library and administrative systems and, via the Web, global collaborations and access to information worldwide. The EA2 infrastructure will permit immediate implementation of these trusted exchanges.”

Representatives serving on the Task Force include:
February 6, 2007
Inter-Organizational Task Force to Advance Electronic Authentication and Authorization for Higher Education

– American Association of Collegiate Registrars and Admission Officers (AACRAO)
  Nancy Krogh, Registrar, University of Idaho
– Educause
  Steve Worona, Director of Policy and Networking Programs
– Electronic Authentication Partnership (EAP)
  David Temoshok, Director of Identity Policy and Management, U.S. General Services Administration
– IMS Global Learning Consortium
  Rob Abel, CEO
– Internet2/InCommon
  Ken Klingenstein, Director of Internet 2 Middleware Initiative
– Liberty Alliance
  Brett McDowell, Executive Director
– National Association of Student Financial Aid Administrators (NASFAA)
  Ellen Blackmun, Director of Technology Initiatives and Distance Learning
– National Council of Higher Education Loan Programs (NCHELP)/Meteor
  Tim Cameron, Project Manager
– Postsecondary Electronic Standards Council (PESC)
  Charles Leonhardt, Principal Technologist, Georgetown University, Task Force Chair
  Adele Marsh, Vice President of Industry Initiatives, AES, representing the PESC Standards Forum for Education
– Schools Interoperability Framework Association (SIFA)
  Larry Fruth, Executive Director
– State Higher Education Executive Officers (SHEEO)
  Hans L’Orange, Director, SHEEO/NCES Network and Director of Data and Information Management
– U.S. Department of Education
  Charlie Coleman, Director, CIO Application Development, Office of Federal Student Aid (FSA)

The inaugural meeting of the Task Force is set for Tuesday March 6, 2007 at the National Center for Higher Education, One Dupont Circle NW, in Washington, D.C. and will run from 9am – 3pm.
Organizations that are members of any of the eleven associations may send representatives to attend and observe Task Force meetings; and those wishing to attend must register in advance by completing and submitting a Registration Form available at www.PESC.org. The first report from the EA2 Task Force is expected late summer of this year.

About AACRAO
The mission of the American Association of Collegiate Registrars and Admissions Officers (AACRAO) is to provide professional development, guidelines and voluntary standards to be used by higher education officials regarding the best practices in records management, admissions, enrollment management, administrative information technology and student services. It also provides a forum for discussion regarding policy initiation and development, interpretation and implementation at the institutional level and in the global educational community. For more information, please visit www.aacrao.org.

- continued -
About Educause
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. The current membership comprises more than 2,000 colleges, universities, and educational organizations, including 200 corporations, with over 16,500 active members. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C. For more information, please visit www.educause.edu.

About EAP
The Electronic Authentication Partnership is comprised of a wide range of stakeholders, including Federal government agencies, state governments, private sector companies and organizations, public interest groups and trade groups. The goal of the EAP is to provide organizations with a trusted means of relying on digital credentials issued by a variety of e-authentication systems. The EAP welcomes any public or private sector organization. For more information please visit www.eapartnership.org.

About Georgetown University
Founded in 1789, the same year the U.S. Constitution took effect, Georgetown University is the nation's oldest Catholic and Jesuit university. Today, Georgetown is a major international research university that embodies its founding principles in the diversity of our students, faculty, and staff, our commitment to justice and the common good, our intellectual openness, and our international character. For more information, please visit www.georgetown.edu.

About IMS
IMS/GLC is the leading advocacy group encouraging the growth and impact of learning technology worldwide. IMS/GLC is a global, nonprofit, member organization that provides leadership in shaping and growing the learning industry through community development of standards, promotion of innovation, and research into best practices. For more information, please visit www.imsglobal.org.

About Internet2
Internet2 is the foremost U.S. advanced networking consortium. Led by the research and education community since 1996, Internet2 promotes the missions of its members by providing both leading-edge network capabilities and unique partnership opportunities that together facilitate the development, deployment and use of revolutionary Internet technologies. Internet2 brings the U.S. research and academic community together with technology leaders from industry, government and the international community to undertake collaborative efforts that have a fundamental impact on tomorrow's Internet. For more information, please visit http://www.internet2.edu/.

About Liberty Alliance
The vision of Liberty Alliance is to enable a networked world based on open standards where consumers, citizens, businesses and governments can more easily conduct online transactions while protecting the privacy and security of identity information. This world, where devices and identities of all kinds are linked by federation and protected by universal strong authentication, is being built today with Liberty's open identity standards, business and deployment guidelines and best practices for managing privacy. For more information, please visit www.projectliberty.org.

About NCHELP
Based in Washington, DC, the National Council of Higher Education Loan Programs, Inc. (NCHELP) represents a nationwide network of guaranty agencies, secondary markets, lenders, loan servicers, collectors, schools and other organizations involved in the administration of the Federal Family Education Loan Program (FFELP). Since its founding, NCHELP has represented its members on public policy and regulatory issues with the legislative and executive branches of the federal government and has fostered the standardization of exchanging loan information electronically, through oversight of the Electronic Standards Committee (ESC) and the Meteor project; making loan application, delivery, and inquiry processes easier, faster, and more efficient. For more information, please visit www.nchelp.org.

About NASFAA
The National Association of Student Financial Aid Administrators (NASFAA) is a nonprofit membership organization that represents more than 12,000 financial aid professionals at nearly 3,000 colleges, universities and career schools across the country. Based in Washington, D.C., NASFAA is the only national association with a primary focus on student aid legislation, regulatory analysis, and training for financial aid administrators. Each year, members help more than 8 million students receive funding for postsecondary education. For more information, please visit www.nasfaa.org.

- continued -
About PESC
Established in 1997 and located in Washington, D.C., the Postsecondary Electronic Standards Council (PESC) is a non-profit, community-based, umbrella association of colleges and universities; professional and commercial organizations; data, software and service providers; and state and federal government agencies. PESC’s mission is to lead the establishment and adoption of data exchange standards in education. The goals of the mission are to enable the improvement of institutional performance and foster collaboration across educational communities in order to lower costs, improve service, and attain system interoperability. For more information, please visit www.pesc.org.

About SHEEO
The State Higher Education Executive Officers (SHEEO) is a nonprofit, nationwide association of the chief executive officers serving statewide coordinating boards and governing boards of postsecondary education. Created in 1954 by the executive officers of nine of the ten statewide higher education boards then in existence, SHEEO’s current members are the chief executive officers serving 26 statewide governing boards and 30 statewide coordinating boards of higher education. For more information, please visit www.sheeo.org.

About SIFA
The Schools Interoperability Framework Association (SIFA) is a unique, non-profit collaboration composed of over 400 schools, districts, states, the U.S. and international government agencies, software vendors and consultants who collectively define the rules and regulations for educational software data interoperability. The SIF Specification enables diverse applications to interact and share data efficiently, reliably, and securely regardless of the platform hosting those applications. SIFA has united these education technology end users and providers in an unprecedented effort to give teachers more time to do what they do best: teach. For more information, please visit www.sifinfo.org.

About US Department of Education
The Department of Education was created in 1980 by combining offices from several federal agencies. Its original directive remains its mission today — to ensure equal access to education and to promote educational excellence throughout the nation. Its 4,500 employees and $71.5 billion budget are dedicated to: establishing policies on federal financial aid for education and distributing as well as monitoring those funds; collecting data on America's schools and disseminating research; focusing national attention on key educational issues; prohibiting discrimination and ensuring equal access to education. For more information, please visit www.ed.gov.
Purpose and Goals
PESC e-Authentication/e-Authorization (EA2) Task Force

The Opportunity

Over the past few years the technology for exchanging data among colleges and universities and with their suppliers has matured. Web services technology provides industry standard Internet-based communications based on XML messages. Security is available through PKI, SAML, and, for colleges and universities’ unique requirements, Shibboleth technology.

The volume of these data exchanges is increasing sharply as more students take courses in multiple institutions, employers require additional documentation of educational experience, education financing has become more widely used and more complex, faculty and student rely more on electronic publications, and colleges and universities offer a spectrum of courses, methods of teaching and learning, and learning environments to match needs of the knowledge economy. In addition, people’s experiences with online financial, information, and purchasing services raise expectations of increasing quality of service from colleges and universities.

As an “industry”, however, postsecondary education has not yet achieved the improvements in service and lower costs that other industries have. With currently available technology, the opportunity now exists to “put the pieces together” to attain the commonality that would drive implementations beyond the “tipping point.” Many believe that reaching “network economies” would benefit colleges and universities and their consumers and suppliers.

The Task Force will focus on this opportunity.

The Goal of the Task Force

The goal of the Task Force is to improve service, lower unit costs, and ensure security through the implementation of e-Authentication and e-Authorization technology and practices. The
result is a common e-Authentication/e-Authorization framework for data exchanges that cooperating parties can implement to support the broader goal.

This requires common, detailed, and unambiguous profiles for existing specifications and standards, perhaps some extensions of existing standards and practices to meet specific needs of postsecondary education; and rationale for priorities, choices, and recommendations that demonstrate feasibility, economies, and sustainability.¹

The Task Force may also recommend specific implementation efforts that would support the broader goal and encourage participation and sponsorship of this work.

**Perspectives**

The work of standards-setting organizations and their early implementers will be reviewed for functionality and judged on their potential benefits to higher education and, pragmatically, the likelihood they will become de facto “standards.” Early implementations, especially in postsecondary education, whether at that time successful or not, will be the primary source of information for the Task Force. These projects also provide a cadre of experienced practitioners whose expertise can be important to the success of any broader implementations.

Mass implementation of a specification, standard or practice largely depends upon the economics of the implementation of new technology and new processes. Economic analysis, even approximations, will guide Task Force recommendations.²

The implementation of new technology accompanied by new processes imply some reorganization of work, which affects relationships of faculty, staff, students, and the organizations and even broader public that are customers and suppliers to colleges and universities. The likelihood of success of an implementation depends in large part on “feasible” short-term and long-term changes to academic and business processes and practices.

The Task Force will assure the different perspectives are understood and shared with the broader community.

---

¹ Most standards have requirements—IETF uses the terms MUST, REQUIRED, and SHALL for requirements, MAY and OPTIONAL for permitted choices, and SHOULD for some ambiguous situations. These are described in Harvard University’s Scott Bradner’s IETF Requests for Comment 2119 drafted in 1997. It is cited as authoritative in almost all standards-setting in information technology. The term “profile” is now frequently used to provide the additional detail needed to achieve data exchanges. Profiles are often defined for a specific industry. For example, an item description for electronic components may be different from item description for the finance industry.

² Various standard-setting organizations use different terms for their results. The terms specification, standards (ISO, OASIS, IETF), and recommendations (W3C) are all used. The emerging practice is specification or recommendation when widely implemented becomes a “de facto standard” or if adopted by a “standards body” then a published “standard.” The ambiguity is not resolved here.
The Role of the Task Force

The Task Force is aware that their work is a series of steps, all done in cooperation with the larger community of colleges and universities and their suppliers and consumers.

The first step will be sharing knowledge of what has been accomplished. There have been successes in implementing data exchanges. Implementation of the PESC electronic XML transcript is an example. The exchange of student financial aid data using NCHelp specifications and U.S. Department of Education practices is another. Supporting the use of IFX and NACHA-compliant financial transactions are yet others. NCHelp’s Meteor Project in conjunction with the U.S. Department of Education is implementing one of the largest uses of OASIS and Internet2 specifications and technology for transitive trust. All of these are based on W3C specifications.

External to postsecondary, the Liberty Alliance has developed standards for exchange of authentication of consumers or users among suppliers. The U.S. government continues to increase the interoperability of systems and the use of common authentication and authorization technology and practices, primarily by the General Services Administration following work of the National Institute of Standards and Technology (NIST) under guidance of the Office of Management and Budget.

The successes of “supply chains” in postsecondary education already demonstrate the characteristics of a successful common framework for data exchanges; often known only to the few who participated in the development and implementation. In each case it was necessary to make detailed decisions on implementations of a specification—often called a profile and collectively as a framework. Identifying and perhaps further documenting this work would provide context for broader collaboration in the Task Force’s work.

Similarly successes in business and industry and government provide examples of specific implementations and, perhaps more important, accurate forecasts of what will become a de facto standard.

The Task Force will need to identify the opportunities where a framework could be useful. Current efforts to integrate scholarly systems, libraries, and administration may provide opportunities.
There are opportunities that cross the traditional boundaries between the various standards-setting bodies—most represented on the Task Force. The interim result could be a list of these individual opportunities.

The Task Force represents a broad spectrum of expertise and experience. One of the most important contributions will be judgments about feasibility and benefits of these individual opportunities. These judgments yield priorities of feasible implementations and identify the scope of commonality required for a framework.

The framework itself then is the selection of technologies and standards, and the specific details of implementation of specifications and standards—the profiles.

The Task Force can also recommend priorities for implementation.
REGISTRATION FORM

E-Authentication/E-Authorization (EA2) Task Force Meeting

National Center for Higher Education
One Dupont Circle NW
Conference Room A
Washington, D.C. 20036
March 6, 2007
9:00am – 3:00pm

Attendee Full Name

Title and Organization

Street Address

City, State and Zip

Phone    Fax    E-mail Address

Affiliated Task Force Association

Please complete this form and return it to PESC:

Postsecondary Electronic Standards Council
One Dupont Circle NW
Suite 520
Washington DC 20036
Fax: 202-872-8857
Email: Sessa@PESC.org

WWW.PESC.ORG