Postsecondary Electronic Standards Council • www.PESC.org Vol. 3 Issue 7, August 2004

# the Standard

news and commentary on technology and standards in postsecondary education

## Inside



POSTSECONDARY Electronic Standards Council

One Dupont Circle, Suite 520
Washington, D.C. 20036

Executive Director
Michael Sessa
*Sessa@PESC.org*

Editor
Heidi L. Weber
*hlweber59@verizon.com*

The Standard is the electronic newsletter published monthly by The Postsecondary Electronic Standards Council (PESC). The Standard covers news and events that impact information technology and data exchange; and promotes PESC's goals of improving service, controlling costs, and attaining interoperability within higher education. For information about subscriptions, advertising, and article submissions, please visit www.PESC.org. 

## Assembly on the State of e-Authentication in Higher Education

BY JIM FARMER

In his opening remarks, PESC Executive Director Michael Sessa said he wanted colleges and universities to be aware of information standards that could benefit higher education and appreciated the speakers' willingness to share this information with the higher education community. At the August 20th event, speakers in fact provided real-world solutions to authentication and authorization needs of colleges and universities.

At the end of the intense day, Sessa said, "Today we have heard about real solutions to real problems and we have heard about work that needs to be done. The great news is that standards are progressing and the biggest value is realized with the implementation of them. We must also ensure that we focus on developing policy for the use of the technology."

The Assembly was held in partnership between the U.S. Department of Education and PESC with sponsorship from Sungard SCT and was held the day following the Department's Software Developers Conference. More than 140 representatives of colleges and universities, software sup-

**See Assembly,** Page 2

## Register NOW!

### Fall 2004 Workgroup Summit

Registration for PESC's Fall 2004 Workgroup Summit is now available! While registration is free, space is limited, so visit www.PESC.org and register online now. Hotel reservations can be made by contacting the Marriott in Newport Beach directly at 949-640-4000. Our room rate is $125 plus tax. Please use the group name "PESC Workgroup" when making your reservations. The cut-off date for hotel accommodations is Friday, September 10, 2004.

Note that the Fall 2004 Workgroup Summit starts at 1:00pm on Tuesday, October 5, and concludes at 5pm, Wednesday, October 6. PESC will also hold a Membership Meeting on Tuesday morning from 10am – 11:30am.

**Assembly,** From Page 1

pliers, government agencies, and the student financial community attended.

David Temoshok, Director of Identity Policy and Management at the U.S. Government Services Administration (GSA) Office of Government-wide Policy, said the federal government had agreed on a federated system of authentication and authorization. GSA asked for implementation of the SAML 1.0 (Security Assertion Markup Language) from OASIS (Organization for Advancement of Structured Information Systems). But he reminded the audience, "Specifying the standard does not guarantee interoperability. We developed the Federal Interoperability Laboratory to ensure the software products we offer to federal departments and agencies would interoperate." Five software suppliers have been approved; about 20 are in process. Approval is required before software can be purchased by federal departments.

The federal government is implementing a four-level assurance and risk schema for identity. Application systems are being classified for the level of risk that is acceptable and the level of assurance that is required; NIST has provided guidance on hardware, software, and procedures necessary to support each level of assurance. The Office of Management and Budget (OMB) mandated the schema by OMB Federal Policy Notice M-04-04 in December 2003. These are the same levels of assurance used for Federal PKI since early 2002 and similar to those used in the Meteor Project.

The federal government expects to also support SAML 1.1 and 2.0 when completed, the Liberty Alliance, and Shibboleth using a protocol translator now under development. Responding later to a question, the protocol translator will not be open source software.

A major issue for the federal government is to develop trust relationships with non-government entities, which is now being developed through the Electronic Authentication Partnership (EAP). GSA, PESC, and a number of major organizations are participating in the EAP. The USA Patriot Act requires an increased level of assurance when a bank account is opened. This gives banking credentials a medium level of assurance. In a February 2004 presentation to federal departments, GSA described how citizens will be able to access federal information resources and transact business using their bank card and PIN for authentication.

Mr. Temoshok said GSA would like to have a single set of agreements and is depending upon the Electronic Authentication Partnership to have these standard agreements in place by October. If EAP is unable to reach agreement, GSA will offer an agreement and accept those firms that are willing to comply.

According to Dave Edstrom, Technical Director & Chief Technologist, Sun Microsystems, Inc., the Liberty Alliance arose from a common need for one business to use the identification credentials from another business to identify users and customers without exchanging any information not needed and not authorized by the owner. The Liberty Alliance is often explained by using your airline frequent flyer identification to rent a car, purchase a book, or book a hotel reservation. In each case the firm providing the product or service "trusts" the airline authentication. The Liberty Alliance work continues and nine software products implemented the Liberty Alliance authentication by December 2003. Many firms will accept Liberty Alliance authentication at the end of 2004 or the first quarter of 2005.

Based on his recent experience at Boston College, IBM executive consultant Bernie Gleason said the simple photo identification card may no longer be sufficient for many transactions. Biometrics may be required to establish the link between the user and the credential. He cited the University of Miami as a lead university with a goal of becoming one of the "Most Trusted Universities." Mr. Gleason was an early advocate of "transitive trust" implemented in the Meteor Project.

**See Assembly,** Page 3

## **Assembly,** From Page 2

David Yakimishak described on-line journal service JSTOR as a "Shibboleth Target." Although IP addressing—that numeric value that identifies your computer to the Internet—is used 90% of the time to establish the user with a particular college or university , this may not be sufficient in the future. Mr. Yakimishak said the inconvenience of having to be on the campus network or the insecurity of using a proxy for off-campus access was still marginally acceptable to the journal publishers, but was not as secure as many would like and does not provide credentials that could differentiate the authorization of one campus user from another. Mr. Yakimishak observed that librarians prefer to make all information resources equally available to all students and all faculty. For additional security while maintaining the user's anonymity, JSTOR has begun support for Shibboleth for authorizing access to JSTOR journals.

JSTOR has 2,105 participating libraries with journals from 264 publishers providing access to 15, 342, 962 pages providing more than 19 million journal pages per month to a purposefully unknown number of users.

A conference participant noted the United Kingdom has a policy of migrating from its current nationally centralized Athens system to Shibboleth federation over the next several years. Some are participating in the JSTOR pilot and others are expected to join when current software development projects are completed.

Yale University's Howard Gilbert reminded the conferees that the purpose of authentication was to solve a university problem. He described a portal as "the Network version of what Universities have always done, so we better learn how to do this right or we will become obsolete." He said we are at "ground zero in the authentication train wreck. Users may have different methods of authentication, data sources may have different methods of authorization, and we can change some information sources, but at some point we have to accommodate legacy systems or lose their content." He pointed out that passwords are "(sometimes) too large and obscure to remember, different for every service, and should not written down anywhere. But the truth is we use the same passwords if we can and write them on a note posted on our computer." Yale developed and uses the Central Authentication System, popularly known as "CAS" with their implementation of JA-SIG's uPortal. "Other places will make other choices." But Yale also wanted the federation capabilities of Shibboleth and are now implementing Shibboleth with CAS in supporting their portal. Mr. Gilbert explains this by saying a Yale logon can be used to access information resources at UCLA because "UCLA trusts the Yale credential."

Mr. Gilbert continued, "the perfect is the enemy of the better." He believes that computer programmers often fail to keep university's needs in mind. As he had said at the uPortal Developers Meeting in St. Johns, "I was hired to solve Yale's problems, not to develop code that impresses another programmer." And the record at Yale support's his view. The Yale University CAS authentication system is now employed at more than 100 colleges and universities, not because of marketing, but because it effectively and efficiently solves the Web single sign-on problem. Yale has been a major contributor to then uPortal project.

His remark is especially important when a problem, such as authentication, has so many political, economic, legal, and technical trade-offs. Often developers wait in fear of not doing the "perfect" and risk-free thing, or focus only on "improving the technology" rather than the messy real-world problem.

University of Southern California Associate Registrar Robert Morley reminded participants that the university constituency was larger than faculty, staff, and students. It includes those making inquiries and search, applicants, admissions, residents and distance learners, alumni, donors, and many combinations. This implies different levels of risk and assurance and different needs for credentials. He pointed out that federal requirements—FERPA, Gramm–Leach–Bliley Act, and now California's restriction on the use of

**See Assembly,** Page 4

**Assembly,** From Page 3

Social Security number—SB 168—and information protection—SB 1386—place demanding requirements for authentication and authorization. USC is looking to Shibboleth and Liberty Alliance to provide answers to their needs.

Scott Cantor gave a "power presentation" on OASIS SAML, the Liberty Alliance Specifications, and Shibboleth. Mr. Cantor has been a principal author or advisor to all three and principal software developer for the widely used OpenSAML software. His advice can be summarized saying:

- Use SAML 1.1 – it fixes some problems with 1.0 and works with Liberty Alliance. SAML 2.0 will be even more complete and should be available soon.
- Be prepared to support Shibboleth (for reasons "power-implementer" David Yakimishak suggested).
- Integrate with Liberty Alliance.
- Know there is some major implementation work if WS-Security is used with Web messaging (SOAP primarily).

The good news is the coordination between the three major efforts will converge in the near future. All use SAML assertions. "There is no need to wait for Web single sign-on." Shibboleth implementations are being tested and the portal version will be available soon. (The London School of Economics is the lead in this JISC-supported implementation).

Echoing David Temoshok's advice, Mr. Cantor said now policies need to be in place so the technology can be used.

AES' Adele Marsh reminded the audience that the Meteor Project has three years of experience using Shibboleth for authentication and authorization, assigning levels of assurance to identification credentials, federating authentication, using real-time Web messages, encrypting data between user and source, and federating and reconciling data from many sources. The Meteor Project was prototyped in January 2001. The next phase was "developing trust" among the competing lenders and servicers to share data among themselves, with financial aid advisors, and now student borrowers. Then the algorithms for combining data from several different sources to present in various formats to users were needed. All of this was based on then-available draft standards or early working papers. The system has now been in service more than two years with growing traffic volumes.

The Meteor Project may be one of the best examples of Howard Gilbert's "nice set of cups from the Pottery Barn"(versus waiting for the perfect solution) in its use of technology, collaborative work of competitors for the benefit of students and financial aid administrators, and the trust network it developed; a source of real-world experience that could guide future efforts.

Mark Jones from the National Student Clearinghouse (NSC) illustrated, perhaps unintentionally, the sharp difference between business and higher education. The Clearinghouse has developed open standards real-time data exchanges with employers, lenders, and other authorized users of student data. But NSC relies almost totally on periodic bulk file transfers of data from colleges and universities. He also observed that digital certificates are now used to authenticate assertions in web messages and to encrypt or sign documents. NSC has the technology and policies from the Corporation for Research and Education Networks (CREN), but so far there has been any demand for these certificates. (Most colleges and universities generate their own certificates which means the certificate cannot be authenticated as valid). He also noted there has been no demand for personal digital certificates, but if there was NSC would be able to provide that service.

Mike Sessa closed the meeting by thanking all speakers and attendees and by saying the presentations would be available at the PESC Website www.PESC.org. Participant evaluations strongly indicated that this kind of summary presentation was very valuable to the colleges and universities and suggested a more technical supplementary presentation for

# OCC Issues Guidance on Electronic Records

By Shelly Repp
NCHELP

The Comptroller of the Currency in June issued an advisory letter on electronic record keeping. The OCC, which regulates national banks, states that while the federal E-SIGN Act changed the legal framework for electronic records, it does not resolve all legal and practical issues regarding electronic records.

The OCC states that banks need to carefully plan their implementation and operation of electronic record systems to ensure that they meet functional and regulatory requirements. The OCC acknowledges that neither the E-SIGN Act nor any banking agency has established minimum standards in such areas as accuracy, record integrity and accessibility and advises that, until more specific standards are developed, banks should ensure that their electronic record systems are adequate to support litigation, audits and controls, bank supervision and regulatory compliance.

The OCC guidance places special focus on the first of these topics, emphasizing that electronic records must be admissible as evidence in a legal proceeding. The guidance notes that electronic documents with electronic signatures may pose special challenges in this regard. The OCC states that courts are continuing to develop precedent in this area, and refers the reader to the Federal Rules of Evidence (particularly Rule 1001(3)). That rule provides that "if data are stored in a computer

**See OCC,** Page 6

## PESC Fall 2004 Membership Meeting

Please be advised that a meeting of the PESC Membership has been scheduled for Tuesday, October 5, 2004 at 10:00 am - 11:30 a.m. This meeting will be held in Newport Beach, CA at the Newport Beach Marriott immediately before PESC's Workgroup Summit which kicks off on the same day at 1:00pm.

Tentatively scheduled for the agenda at this time:

- Board Update on PESC's Strategic Direction
  Elections for the Standards Forum Steering Committee
- Roll out of Standards Forum Policies and Procedures
- Roll out of the XML Registry and Repository

Also note that PESC is hosting a Membership Luncheon immediately following the Membership Meeting. Please RSVP directly to Ane Johnson, PESC's Membership Coordinator at Johnson@PESC.org.

## Steering Committee Nominations Now Open

As elections for the Steering Committee will be held during the Membership Meeting, we are now accepting nominations for the Steering Committee, which is a 5 member body that leads and provides oversight for the Standards Forum for Education. Those interested in nominating or in serving should send the nominees name, title, organization, and a brief bio to the attention of Michael Sessa, PESC Executive Director, One Dupont Circle NW, Suite 520, Washington DC 20036. Email nominations can also be submitted to Sessa@PESC.org. Nominations will be closed COB Friday September 17, 2004. Note that representatives must be from organizations that are MEMBERS of PESC. Proxy ballots will then be issued Monday September 20, 2004.

We encourage all of PESC members and affiliates to attend as Membership Meetings are your chance to influence the direction of your organization! If you have yet to register for the free Workgroup Summit in Newport Beach, please visit www.PESC.org.

We look forward to seeing you in October!

**Milestone,** From Page 5

or similar devise, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'". Under this rule, affidavits and/or testimony may be needed to prove that the authenticity and accuracy of an electronic record (including an e-signed record). It is noteworthy that the guidance states that the electronic record must be "readable." Does this mean that the electronic record does not need to be an exact copy of the original record?

The OCC guidance also states that banks need to provide for continued accessibility to the electronic record despite future changes in record systems. Thus, in proving the authenticity and accuracy of an electronic record, the technology and processes in effect at the time the record was created may need to be proven even though those systems may have been changed.

A couple of questions come to mind in reading the OCC guidance. First, why did the OCC feel it important to issue this cautionary guidance now, more than 3½ years following passage of the E-SIGN Act? Second, why did they emphasize the need to be concerned over the admissibility of electronic records in litigation?

The guidance has relevance for student loan participants, particularly for private loans. While the guidance also applies to a bank's FFELP activities, the Department of Education's (ED's) specific guidance that was issued in April 2001 (the "Standards for Electronic Signatures in Electronic Student Loan Transactions") is of at least of equal importance. ED's standards provide a framework for addressing electronic record keeping issues for this asset class. ED has gone so far as to state that a lender whose processes for electronic signatures and related electronic records satisfy these standards will be protected from loss of federal benefits even if a loan is determined to be unenforceable based on those processes. Banks should be able to argue that they have met the OCC requirements if their electronic record systems comply with the more specific standards in the ED guidance. It should be noted, however, that under ED's standards a lender must provide a transferee with an affidavit or certification, and witness testimony, to ensure the admissibility of the loan records in a legal proceeding. The full import of this standard is not completely clear (what happens if the record is not found to be admissible?), but it reflects a similar concern over admissibility.

NCHELP has formed an E-Sign Electronic Records Exchange Workgroup to look at the data storage and data transportation issues that involve e-signed loans. Specifically, the workgroup looks to make recommendations on the operational methods and technological solutions to standardize: data exchange methods, serial MPN tracking, collateral exchange for claims, support for the Common Claims Initiative (CCI), and the format in which e-sign information is stored and exchanged between data traders. Anyone interested in participating should contact Mark Putman at mputman@nchelp.org.

## In The News

On August 09, 2004, Microsoft announced that it will provide support for WSRP, a standard that allows one portal to consume a portlet running on a remote portal, using Web services protocols, according to a Gartner Report article. For additional information on WSRP and Microsoft's involvement visit http://www4.gartner.com/DisplayDocument?doc_cd=122373

In a move to get more users to access the Web via mobile devices, the W3C and the Open Mobile Alliance (OMA) have agreed to collaborate on specifications. The W3C and OMA, which develops standards for mobile data services, will share technical information and specs to help provide solid, workable standards that benefit developers, product and service providers and users. The groups will hold meetings together to discuss each other's progress. For additional information visit http://www.internetnews.com/dev-news/article.php/3388211

# Technology Tidbits

*and Standards Snippets*

■ **According to a draft report on a survey, of 4,374 freshmen and seniors at 13 colleges of all types, was conducted this year by the Educause Center for Applied Research, 48.5 percent of respondents said the biggest benefit of classroom technology is convenience**, such as the ability to check grades online, states a Chronicle of Higher Education article. Only 12.7 percent of the students said improved learning was the greatest benefit, and 3.7 percent said technology provided no benefit at all in the classroom. The final report on the survey is set to be released this fall, and will be available for sale at www.educause.org.

■ **The Student and Exchange Visitor Information System (SEVIS) has launched a Web site, http://www.ice.gov/graphics/sevis/, with information for schools and programs, students, and exchange visitors.** SEVIS is also "celebrating" its one-year anniversary. In the SEVIS program's first year, 8,737 schools and exchange visitor programs, representing more than 9,500 campuses have been certified to participate in the program. As of July 2004, there are more than 770,000 students and exchange visitors (F-1, M-1 and J-1 visa categories) approved to study in the United States whose data is being managed by SEVIS. In addition, SEVIS maintains records on more than 100,000 dependents of students and exchange visitors.

UT Austin Internet Server
**'SPEEDEs' Along**

July 2004 volume included:

- 41,954 TS130 transcripts
  Most ever in any one month.
- 36,743 TS131 acknowledgements
- 6.077 TS997 Functional acknowledgements
- 11,154 TS189 Admission Applications
- 2,705 TS138 test score reports
- 113,222 total transactions

■ **Indiana University and the University of Hawaii are leading an effort to build a free, open-source alternative to costly admininstrative solutions**, according to a recent Chronicle of Higher Education article. The institutions plan to devote more than $2.5-million in staff time and resources to the project, which is called Kuali. The software is aimed at helping to manage accounting, billing, e-com-

merce, budget planning, and other campus functions. The article can be accessed at http://chronicle.com /free/2004/08/2004083002n.htm

■ **The Interactive Financial eXchange (IFX) Forum has been working to develop a business message specification to satisfy the need for a community vocabulary and messaging specification in the retail and commercial banking arenas.** But the more than seven years of work has resulted in much more than just a community vocabulary. IFX provides design rules and a framework to successfully achieve consistency and interoperability, within a bank and between a bank and other entities. IFX provides many design benefits for XML developers in the financial industry. For additional information visit http://www.syscon.com/ story/?storyid=45790&DE=1

■ **Microsoft recently withdrew from a United Nations software standards group for commerce, citing 'business reasons.'** Earlier this year, Microsoft's participation had created controversy within the group, which is attempting to define standards for creating a new generation of Internet services to automate buying and selling through networks of computers, according to CNET article. Microsoft's with-

## FSA Moves to XML

On August 6, 2004, the General Manager, FSA Application, School Eligibility and Delivery Services announced the COD Full Participant Requirement for 2005-2006 Award Year.

FSA reminds the financial aid community that ***all*** schools must be Common Origination and Disbursement (COD) Full Participants beginning with the 2005-2006 Award Year. This means that ***all*** schools must be able to submit 2005-2006 Pell and/or Direct Loan origination and disbursement data to the COD System using the COD Common Record in XML format.

**Note:** FSA recently informed schools in GEN-04-06 that the implementation of the Common Record: ISIR will not be implemented for the 2005-2006 Award Year. The adjustment of the Common Record: ISIR implementation schedule ***does not*** affect the requirement that ***all*** schools must be COD Full Participants beginning with the 2005-2006 Award Year.

For more information or to read the full announcement, please visit http://www.ifap.ed.gov/eannouncements/0806CODFullParticReq0506.html.

drawal stemmed from issues over the control of intellectual property that is being contributed to the standards-setting effort. For more information http://news.com.com/2100-1013_3-5321782.html

■ **OASIS recently approved SAML v2.0 specification as a Committee Draft** and voted to submit the specification documents for public review. Comments are solicited from all interested parties and may be submitted via a web form found at http://www.oasis-open.org/committees/security. The public review period will end September 19.

■ **W3C Technical Architecture Group, has issued the last call working draft of its "Architecture of the World Wide Web, First Edition.** "The World Wide Web is an information space of interrelated resources. This information space is the basis of, and is shared by, a number of information systems. Within each of these systems, people and software retrieve, create, display, analyze, relate, and reason about resources. Web architecture defines the information space in terms of identification of resources, representation of resource state, and the protocols that support the interaction between agents and resources in the space. Web architecture is influenced by social requirements and software engineering principles. These lead to design choices and constraints on the behavior of systems that use the Web in order to achieve desired properties of the shared information space: efficiency, scalability, and the potential for indefinite growth across languages, cultures, and media. Good practice by agents in the system is also important to the success of the system. This document reflects the three bases of Web architecture: identification, interaction, and representation." To access the document in its entirety http://www.w3.org/TR/2004/ WD-webarch-20040816/

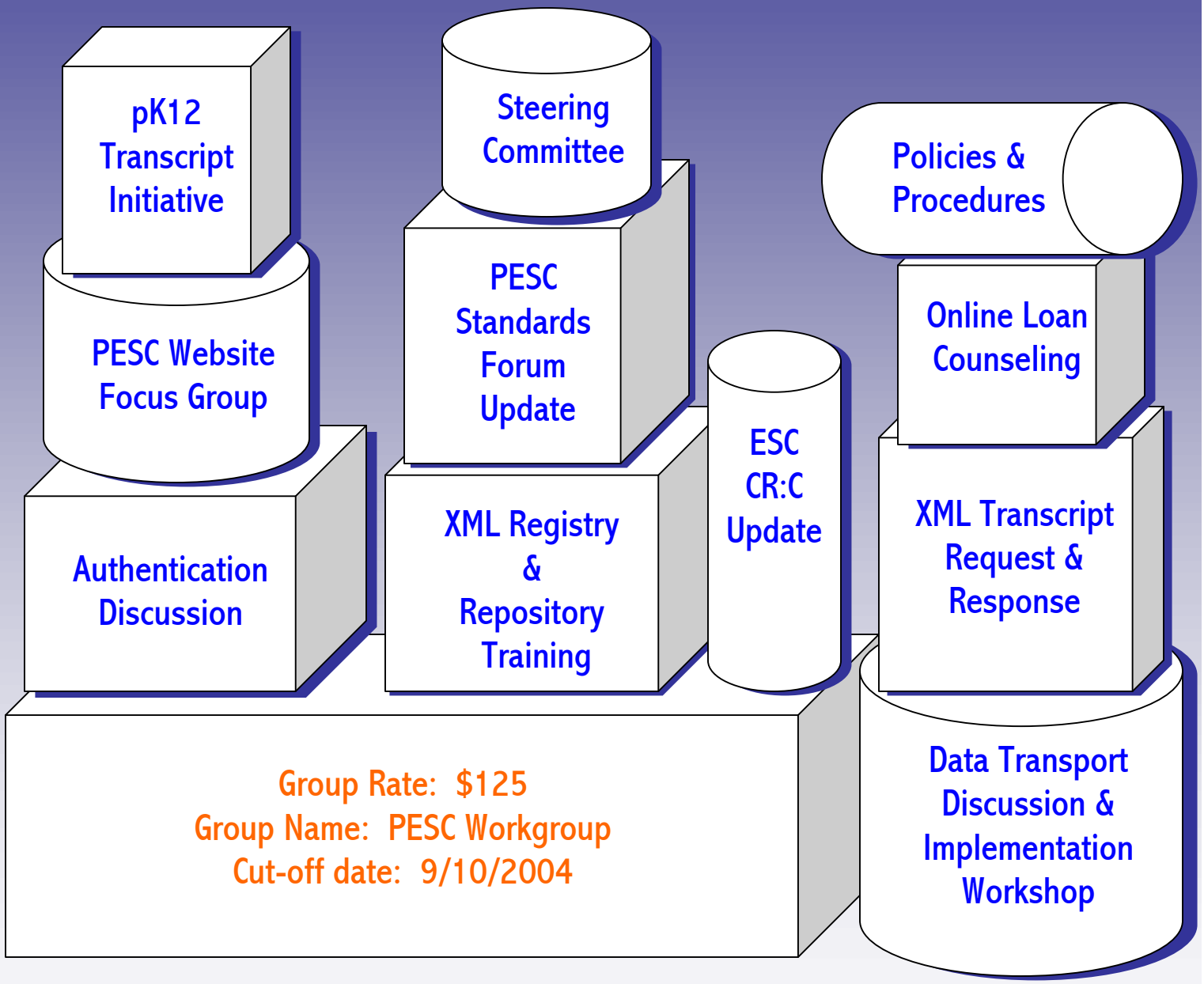
■ On August 09, 2004, **Microsoft announced that it will provide support for WSRP, a standard that allows one portal to consume a portlet running on a remote portal**, using Web services protocols, according to a Gartner Report article. For additional information on WSRP and Microsoft's involvement visit http://www4.gartner.com/DisplayDocument?doc_cd=122373.

■ **In a move to get more users to access the Web via mobile devices, the W3C and the Open Mobile Alliance (OMA) have agreed to collaborate on specifications.** The W3C and OMA, which develops standards for mobile data services, will share technical information and specs to help provide solid, workable standards that benefit developers, product and service providers and users. The groups will hold meetings together to discuss each other's progress. For additional information visit http://www.internetnews.com/devnews/article.php/3388211

NEWPORT BEACH MARRIOTT ~ NEWPORT BEACH, CA ~ 949-640-4000

TUESDAY OCTOBER 5, 2004 – WEDNESDAY OCTOBER 6, 2004

# Workgroup Summit




Group Rate: $125

Group Name: PESC Workgroup

Cut-off date: 9/10/2004

*Online Registration Available Now at:*

## www.PESC.org

POSTSECONDARY Electronic Standards Council