Recommendations of the PESC Electronic Authentication and Authorization (EA2) Task Force for the PESC Board of Directors Regarding the Relationship between PESC and InCommon

Executive summary

The EA2 working group recommends that PESC and InCommon form a strategic partnership to endorse, create, and promote the adoption of standards that will enhance higher education and further achieve shared goals of both groups. A Memo of Understanding drafted by a joint task force will document the intent and responsibilities of this partnership. PESC's mission of enabling “cost-effective connectivity between data systems to accelerate performance and service”, simplifying “data access and research”, and improving “data quality along the higher education lifecycle”1, is closely aligned with InCommon's mission “to create … a community-based common trust fabric sufficient to enable participants to make appropriate decisions about the release of identity information and the control of access to protected online resources.”2

The InCommon Federation (and Certificate Service), which is the community-based common trust fabric referred to in their mission, has over 200 members, and membership trends indicate that over 50% of all students in higher education in the United States will be attending member schools by the end of the 2011is calendar year.

To show our support of the work that InCommon is doing, the EA2 working group recommends that InCommon be granted the PESC Seal of Approval in recognition of the synergy between the two organizations and shared goals.

The attributes about individuals that are exchanged between identity providers and service providers within the Federation are defined in the eduPerson Object Class, a data standard developed and maintained by the MACE (Middleware Architecture Committee for Education) Directories working group. Established in 2000 through work with the Internet2 Middleware Initiative, the eduPerson Object Class has been widely adopted internationally and is used as the basis for identity information exchange in several countries, including France, Spain, Norway, the United Kingdom, and the United States. The EA2 working group recommends the adoption of the eduPerson standard as a PESC standard. 3

PESC supports protected web portals, including the EdUnify portal and the PESC presence on edu1world. As a second step in the process of partnership, The EA2 working group advocates sponsoring EdUnify into the InCommon Federation, and protecting access to it with Shibboleth (the open source Security Assertion Markup Language (SAML) compliant Federated Single-Sign-On solution produced by Internet2) as a primary option for authenticating to PESC managed web portals. The working group further recommends that PESC encourage the edu1world portal to act similarly. This will serve as an example to member institutions and vendors.

1 http://www.pesc.org/interior.php?page_id=156
2 http://www.incommon.org/about.html
3 http://middleware.internet2.edu/eduperson/
As another future step, there is an opportunity to establish an Identity Provider for PESC vendor members, which would allow these vendors access to the Federation to support their higher education clients. This would encourage development of Federation-able, SAML-aware applications.

Enterprises gain access to the InCommon Federation partner's and member's services through the use of Identity Providers (IdP's) that are typically installed at each institution and are connected to the institution's identity store, from which authoritative information can be obtained about members of the institution. Vendor members of PESC would benefit from the establishment of a PESC IdP, which would give them the incentive and opportunity to build and market SAML aware applications. Joining InCommon, or any Federation, requires legal hurdles to be overcome, and smaller institutions of higher education may also be inhibited by a lack of technical resources required to install, configure, and maintain an IdP. While there are several InCommon Affiliate commercial organizations that provide Identity Provider services to enterprises not able or willing to establish their own, a PESC IdP would provide cost-effective connectivity between data systems and improve data quality by offering short-term solutions to these smaller schools. Further study is required to determine if the existing organizations in this field are sufficient, or if this is a place where PESC could make a contribution.

Finally, in order for some data to be shared between schools, government agencies, parents, students, and vendors, it is often necessary to satisfy pre-defined Levels of Assurance (LOA's). These LOA's were introduced in the United States by NIST 800-63, and range from 1 to 4, with 1 being the least secure and 4 being suitable for top-secret military work. InCommon has defined LOA's of Bronze and Silver, and are “consistent with the federal government's levels of assurance 1 and 2.” Unfortunately, meeting even these requirements has proved daunting, despite requirements to do so. Because the lack of compliance with these LOA's impedes data access and research and data quality, working towards widespread adoption of InCommon LOA Bronze and Silver is directly aligned within the mission of PESC. We propose that PESC play an active role in supporting PESC members in their efforts to achieve Bronze and Silver levels of assurance by providing consulting services to any member institution seeking to achieve these levels of assurance in a compliant manner. EA2 recommends and supports these actions to further improve all aspects of security as PESC succeeds in promoting Common Data Standards and inter- and intra- institution communication.

4 http://www.incommon.org/assurance/
Background

Removing the barriers preventing access to longitudinal data and data alignment along the entire student lifecycle requires addressing the issues surrounding the authentication of all actors at a level that meets the requirements of the Federal Government as defined by LOA. The issues surrounding authorization of these persons to access data they need and are allowed access to by law and regulation while protecting data from unauthorized access must be resolved. At the end of this document are example use cases describing how real time access to data and information across and within each education enterprise would facilitate smoother and more secure communications between all individuals and groups in education. These use cases are written in a relaxed and occasionally comical style to make them as accessible as possible, but their messages are powerful. OASIS\(^5\) has played a key role in developing and promoting the Security Assertion Markup Language (SAML)\(^6\), and Internet2's\(^7\) primary open source implementation Shibboleth\(^8\). InCommon is a Federation of Higher Education institutions that enables these products to work across higher education enterprises by establishing in advance the trust relationships needed between institutions. Once this trust is established, vendors can confidently build to these standards, allowing a much higher level of interaction between all members of the community. The body of this document describes the critical importance of the growth of InCommon membership and adoption towards accomplishing all of PESC's stated goals.

InCommon is a Federation of colleges and universities and their partners who have agreed to a legal agreement, operating practices, and technical standards of the federation. Technical interoperability is achieved by enabling institutions to authenticate their users and then pass information (i.e. “attributes”) about users to service providers for authorization. The eduPerson Object Class defines the collection of attributes exchanged. The use of this standard is one of the keys to enabling distributed access control.

From the user's perspective, the flow path through the system reflects the following:

- User goes to a web site protected by SAML
- User is redirected to a logon screen provided by the user's current parent institution. The choice of parent institution may be contextual; users may have identity stores at more than one location. Some use cases describe aggregating attributes.
- User then provides their institutional username and password (or whatever token the parent institution uses)
- Attributes about the user are provided to the protected web site. The attributes released need not communicate the identity of the individual. The release of attributes is dependent upon the policies of the parent institution.
- Authorization decisions are made using a mechanism chosen by the web site's administrator. (Note: authorization methods are out of the scope of this discussion, except to note that the SAML mechanism allows for a variety of possibilities, and an institution's choice of authorization mechanisms has no bearing on other institutions)

---

5 http://www.oasis-open.org/home/index.php
6 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
7 http://www.internet2.edu/
8 http://shibboleth.internet2.edu/about.html
InCommon membership currently boasts over 200 colleges and universities, with the goal of 290 by the end of 2011. Because of the size of the member institution, the latter number could represent over 50% of the students in higher education in the United States. Joining InCommon involves a recognition of the benefits of Federation membership, getting the institution legal department to sign off on the agreements, and paying the minimal annual dues. Once applications become available that require higher levels of assurance, the harder part will be meeting these levels. Setting up the Identity Provider that allows users to log in using their home institutions credentials and be able to work on secure systems locally or remotely can be a technology hurdle. Neither meeting a certain level of assurance, or even setting up an Identity Provider are requirements to join InCommon, but until some number of institutions have set up, or connected to, an Identity Provider and met the necessary levels of assurance to use secure applications, vendors have little incentive to make their existing applications or new development “SAML-aware.” It seems clear that InCommon is working towards the level of participation necessary to spur wide spread application support. But institutions can find that setting up an Identity Provider may be technically and politically challenging, and that without vendor applications capable of leveraging the technology the return on investment may be unsatisfactory. The drivers for vendors are increased security, decreased account/user management costs, and assuredness that the people accessing the service are current members of the institutions.

EduPerson\(^9\) is the data standard published by Internet2 and maintained by MACE that seeks to describe commonly shared attributes of a person in the higher education world. Joining InCommon implies adoption of the eduPerson standard, so the resources published will be compatible within the Federation. This common standard allows service providers to know what attributes are reasonable to request from identity providers and identity providers to know what attributes they should maintain and provide.

There are two potential paths that can be taken when sharing data between institutions, either participating institutions batch load their data to a data warehouse, or they set up a standardized mechanism for sharing their data in real time to appropriate persons at appropriate institutions. In the first situation, data often becomes stale, with the currency of the data limited by how frequent batch loads are performed. A batch load of student enrollment done at the end of each add/drop period will not accurately represent students who drop out of school mid semester until the next semester's add/drop and subsequent batch load takes place. The first situation also puts the institution's data in the control of a 3\(^{rd}\) party. The institution depends upon this 3\(^{rd}\) party to enforce regulations. What is the institution's level of exposure if the 3\(^{rd}\) party fails to properly comply with federal regulations? The strength of the legal agreement is the only control the institution has over the data.

The second path allows real-time access to institutional data based upon the privileges awarded the person (or system) requesting the data. The consumer receives a filtered view of the data, as it exists in the requested database at the time of the request. In the case of students enrolled in multiple institutions, a single set of credentials can allow a user to gather all the relevant data for that student across all relevant databases. It becomes entirely the institution's responsibility to

---

9 http://middleware.internet2.edu/eduperson/
enforce regulations, which could be viewed as a negative due to the increased responsibility, but at least the institution has the opportunity to ensure these regulations are enforced to its satisfaction. If money is to be exchanged for data then the institution has the ability to reap the benefits. The institution also has the ability to decide what they will give away for free. For example, some schools prefer to give away transcripts to alumnae, others charge. InCommon and SAML allows for this infrastructure of real-time data communication, and leaves the control of the data in the hands of the institution that is ultimately responsible for it.

**Recommended actions regarding InCommon and EduPerson**

**Endorsement and PESC Seal of Approval**

Growth in SAML and InCommon can only benefit the higher education community. SAML is a standard that directly benefits all elements of higher education, potentially the entire PK20 spectrum. The eduPerson standard is at the core of InCommon's ability to support all aspects of higher education, from research to administration, and all members of the community from administrators to faculty to students to parents, as well as government agencies and PK-12 school districts. The use cases at the end of this document demonstrate the potential value of widespread adoption of InCommon and the eduPerson and SAML standards. Therefore, the EA2 working group strongly recommends that PESC endorse eduPerson and InCommon, and offer eduPerson and/or InCommon the PESC Seal of Approval. The EA2 working group also recommends that PESC adopt eduPerson as a PESC standard. Advertising eduPerson as a PESC standard will clearly state that PESC recommends eduPerson and endorses the maintenance of eduPerson. We recommend that these things be included in the PESC web presence and be announced in press releases.

**Strategic Partnership**

A higher level of achievement, and a huge boost to PESC’s value to the higher education community, would be the creation of a strategic partnership between PESC and InCommon. In a discussion with InCommon representative and UMBC VP and CIO Jack Suess during the February 16th EA2 teleconference, PESC was invited to create a mutually advantageous strategic partnership, which would provide the benefits of InCommon membership without the requirement of paying annual dues. There can be no doubt that the goals of PESC are greatly enhanced by InCommon's work, and there are advantages to both PESC and InCommon to participating in such a partnership.

Mr. Suess discussed two distinct areas where this partnership will be valuable: a PESC Identity Provider that would ease the transition for InCommon members into the Federation; and PESC acting as a consultant to help institutions achieve Bronze and Silver Levels of Assurance as needed. There are other benefits. This move would demonstrate PESC’s commitment to promoting standards in higher education, as PESC acts as a mentor to bring schools that have the will but not the resources to do it themselves. Additionally, while ushering schools into the Federation, this move will increase participation by higher education institutions in PESC. As actual participation in the Federation increases, the vendor community in PESC will have early access to the power of the Federation as they develop new versions of their tools designed to support the vast array of newly possible communications made available by the widespread adoption of the InCommon Federation. The use cases demonstrate the importance of this standard to the future of higher education administration and research.
Shibboleth enable PESC managed web portals

It is important as PESC moves forward on these efforts that the best possible example be set. To that end, it is important that efforts begin immediately to Shibboleth enable PESC web portals. There are already plans in place to add Shibboleth authentication to the EdUnify portal and make it available in the InCommon Federation. PESC should approach the owners of the edu1world portal to begin the process of adding the ability to accept Shibboleth authentication to augment or replace the existing mechanism. Not only will this demonstrate PESC’s determination to support these technologies, it will also make management of these portals that represent PESC to the world more secure.

PESC Identity Provider

The establishment of a PESC Identity Provider for PESC vendor members, in support of PESC's SAML enabled portals, and to act as a transition vehicle for institutions of higher education struggling to establish their own IdP would be mutually beneficial to PESC and InCommon. Vendors will need a way to test SAML and Federation support in new product development, and will need access to provide good customer service. Granting PESC vendor members access to a PESC Identity Provider may lead to increased vendor support for all InCommon activities, to the benefit of InCommon, PESC, and all member institutions. It is not clear yet that a PESC Identity Provider for higher education enterprises would automatically be something that should be pursued, because there are commercial vendors offering this service. However, should it be determined that there is a valid business model for it, a PESC Identity Provider could be offered as a service to PESC members. A PESC Identity Provider would be a secured server hosted and administered by PESC, and made available under predetermined circumstances to PESC member institutions, based upon whatever business model PESC chooses to adopt. The Identity Provider would be connected to subscribing institution's identity stores to enable PESC to provide SAML assertions for institution members on behalf of each institution. These assertions would be identical to the assertions that would be issued by an institution, and would in all ways be indistinguishable from assertions that would come from an installation on the institution's campus. This service will allow the schools that subscribe to InCommon's principles and pay annual dues to InCommon and PESC to gain all the advantages of InCommon without having to host their own Identity Provider. Identities would not be stored on this server, and PESC would not be responsible for member institution's identity management protocols. PESC would only offer SAML assertions based upon the contents of the institution's identity stores.

The advantage of this fast-track approach to getting institutions up and running in a tangible way on InCommon is the potential growth of applications that use SAML for authentication. Until a critical mass of institutions have and use fully functioning Identity Providers, there is reduced incentive for vendors to supply SAML aware applications. Worse still, until InCommon actually fills the standardized authentication vacuum, there remains the risk that institutions will go down a non-standard approach, or choose a less viable standard, putting wide-spread secure communications within higher education in danger.

PESC Level of Assurance (LOA) Consulting

There has been much discussion around levels of assurance in the authentication world. NIST has identified four levels of assurance. InCommon has identified three that map to the first three levels of the NIST standard. One possible role that PESC could perform would be to provide consulting services to assist institutions in the implementation of LOA. The first step might well
be to create a standard describing the qualities each task now being performed by higher education might require, and differentiate levels between different roles that might perform each task. Publishing these standards will help the Federation members to cooperatively agree upon an attribute that would describe which level of assurance each individual has achieved, and describe what actions each institution must take to grant that attribute to each individual.

Summary

The recommendation of the PESC EA2 working group is that PESC should immediately move to forge a strong strategic partnership with InCommon. Part of this strategic partnership would involve public relations and media, part would involve the creation of mutually beneficial standards, and part would involve performing technical activities on the part of PESC. These activities would help InCommon meet their goal of 290 institutions of higher education being members by the end of 2011, and encourage those 290 members to be active in both the Federation and PESC. These activities will help strengthen adoption of PESC standards by further encouraging their implementation across a broad arena of institutions. An active partnership will provide the vendor community within PESC a forum for communication with InCommon, and will give InCommon access to vendors active in higher education, helping to guide the vendor community towards standards and Federation. An active partnership will raise awareness of PESC in the university CIO space. An active partnership will help guide PESC to creating future standards that encourage adoption of a single method of authentication to the exclusion of others, which in turn will encourage wide-spread software development, increased collaboration and communication, and a more satisfying experience for all actors involved in the higher education environment. Finally, these activities will visibly announce to all agencies the exact future PESC and InCommon sees for higher education authentication and authorization standards, allowing agencies that work closely with higher education to develop applications and behaviors accordingly.
Appendix 1 PESC and InCommon Mission Statements

PESC

Mission
Through open and transparent community participation, PESC enables cost-effective connectivity between data systems to accelerate performance and service, to simplify data access and research, and to improve data quality along the higher education lifecycle.

While PESC promotes the implementation and usage of data exchange standards, PESC does not set (create or establish) policies related to privacy and security. Organizations and entities using PESC standards and services should ensure they comply with FERPA and all local, state, federal and international rules on privacy and security as applicable.

Vision
PESC envisions national and international interoperability, that is a trustworthy, inter-connected environment built by and between communities of interest in which data flows seamlessly from one system to another and throughout the entire eco-system when and where needed without compatibility barriers but in a safe, secure, reliable, and efficient manner.

InCommon

The mission of the InCommon Federation is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States. To achieve its mission, InCommon will facilitate development of a community-based common trust fabric sufficient to enable participants to make appropriate decisions about the release of identity information and the control of access to protected online resources. InCommon is intended to enable production-level end-user access to a wide variety of protected resources.

---

10 Available at: http://www.pesc.org/interior.php?page_id=156
11 Available at: http://www.incommon.org/about.html
Appendix 2a: Selected SAML-aware applications in the Federation

The following applications are reported by InCommon as already having at least one Federation-aware application in production at one or more institutions.

Business Functions
-------------------
Benefits
Human Resources System
Career Services
Asset management
Talent management
Visas & INS compliance
Mobile alerts
Travel management
Energy management
Surveys and market analysis
Student loan eligibility verification

Learning and Research
----------------------
Journals (Lots of Content)
Databases and analytical tools
Multi-media access
Homework labs
Quiz tools
Plagiarism detection
Software downloading
Alcohol awareness education
Student travel discounts
Transportation and ride-share services
Course sharing and video streaming
NSF/NIH Grant Submission
Appendix 2b: Specific SAML-aware applications in the Federation

Library Services

Ares (Atlas Systems)
Aeon (Atlas Systems)
BioOne
eBook Library
EBSCO Host
Science Direct (Elsevier)
Scopus (Elsevier)
JSTOR
RefWorks COS
Thomson Reuters Web of Science
WilsonWeb (H.W. Wilson Company)
First Search (OCLC)
OhioLINK
Proquest Classic
Chadwyck-Healy (ProQuest)
CSA Illumina (ProQuest)
Safari Books Online
Alexander Street Press
Cambridge University Press
IEEE
Serials Solutions

Teaching, Learning and Research

Absorb Learning Management System
Cengage Learning
eLMS (e-academy)
ActivityInsight (Digital Measures)
CourseResponse (Digital Measures)
iTunesU (Apple)
TurnItIn (iParadigms)
Learn.com
Dreamspark (Microsoft)
Sum Total LMS
WebAssign
ALEKS
VoiceThread (collaboration)
CTSA wiki (National Institutes of Health)
Appendix 3: Examples of Exchanges of Real-time Data Between and Within Schools, Districts, Colleges, Universities, Government Departments and Agencies, Organizations, and Businesses

The following general examples highlight the importance of furthering the efforts of both InCommon and PESC. Real time data transport in all aspects of education are going to have to replace batch processing as a method for accurately and rapidly assessing the status of all participants in the education arena at all levels, and as the pressure for real time data transport increase, so will the pressure for attribute based authentication and authorization within a robust trust fabric as provided by InCommon. This appendix is a general overview of some critical uses, appendix 4 includes some stories that highlight some examples of these use cases in action.

For two years the federal focus on education data transport has been for accountability. These data, periodically aggregated, are transported as secured data files. However, when suggesting student performance data be transmitted to teachers and higher education faculty, best use requires real-time data exchanges.

Talks began in July 2009 on how this might be best done in collaboration with the Student Interoperability Framework Association’s development of an updated specification for Web Services data transport. The final step is a SIFA Specification Developers Camp 11-12 April in Dallas, Texas. Comments from software development firms at the 19-21 SIFA Conference suggested software implementing the 2.5 version of the SIFA specification would begin to be available Fall 2011.

Collaboration includes the 12 April 2010 “Harmonizing Web Services Data Transport Standards for Teaching, Learning, and Support of Students” initiated by the U.S. Department of Defense’s Advanced Distributed Learning (ADL) Initiative and the subsequent discussions, two meetings of ADL, AICC (Aviation Industry CBT Committee) and LETSI (Learning, Education, Training Standards Initiative), and the SIF Associations Annual Meeting. The focus was on the exchange of data between a learning delivery systems or services and student management systems. This follows the original ADL concept implemented in the SCORM specifications. The primary use was conceived as a student using a simulator or software presenting a course or learning activity with results provided to a learning management system. Higher education representatives were invited to these; only representatives from the Thebes Project participated. Informal meeting between those developing prototypes for ADL, implementations of the LETIS WS run-time specification, and the Thebes project continue.

Implemented Exchanges in Higher/Tertiary Education

There is one real-time administrative networks operating today serving U.S. colleges and universities. The U.S. colleges and universities could participate in the European Higher Education Area network supporting student mobility, but at this time would need to use a server in EHEA.

Since 2001 a network sponsored by the National Center for Higher Education Loan Programs called Meteor provided real-time access to a student’s student loan records (even if the student
did not know where they were serviced). This application was available to financial aid staff and students. Both had to access the network using credentials from a guaranty agency. (NIST Level of Assurance 2 is required; For practical reasons registrars offer only LOA1). The network was developed using the available W3C and OASIS Web Services specifications when the network was implemented. In 2005 and 2006 further applicable standards were developed. Though planned these were not implemented because of the nationalization of servicing of federally guaranteed student loans.

A second network outside the U.S. called RS3G (Rome Student Systems Specification Group, an informal collaboration) began pilot exchanges of student data consistent with the standards for a Web Services-compliant network in 2010 and broad implementation in the 47-country European Higher Education Area begins in 2011. (The European designation came from development of the processes in the European Union. Subsequently other nations, not including Canada or the U.S., have adopted and are supporting the processes). The network could facilitate registration, U.S. financial aid reporting compliance, and student progress data of U.S. students enrolled in a HEA college or university. U.S. institutions will now be able to participate using an RS3G-compliant service center. These processes are not yet supported in U.S. higher education software. Following guidance from the University of Manchester, the network operates at, but has not been certified for U.S. Level of Assurance 2.

Exchanges Among Colleges and Universities

As business processes change to take advantage of information technology advances and to meet student expectations, PESC has a number of specifications that could be used to define the data “payload” exchanged over a protected network. Here are some examples based on three processes; application, transcript, and course catalog.

Transcripts

Historically the University of Texas as operated a server that exchanges transcripts in either the PESC XML format or the earlier EDI (Electronic Data Interchange) format. The server processed 452,249 transactions in January 2011. Most commercial student information systems can process both received and sent transcripts.

This does not include the five servicers that exchange transcripts; some with extensions implemented using proprietary formats. Some real-time data exchanges between colleges and universities and these servicers have been implemented.

Related services include confirming of enrollment, requesting certified transcripts for employers, and automated notices of change in enrollment status. Because confirming enrollment is often required by health and automobile insurance firms to provide reduced rates, employers who pay for employees taking courses, and government agencies, real-time data exchanges are needed to reduce the error in reporting using data that is updated infrequently.
Admissions

Similarly applications for admission are processed using either an institutional process or a servicer for data entry. There are other services using different formats. The specification could be expanded to confirm admission status to a third-party

Catalog Data

A PESC Workgroup has or will complete a specification for inquiry of course catalog data or transferring course catalogs. The Workgroup expects to exchange the digital equivalent of an electronic version of the university or college’s course catalog until a real-time query/response can be implemented. When implemented this will reduce the delay between application for admission and credit for previous work and admission with prior credit as well as reducing the effort required to obtain the catalog data.

Federal Student Assistance

The U.S. Department of Education expects to implement real-time transaction access to the National Student Loan Data System (NSLDS) for a student’s financial aid status, awards for concurrent enrollment, and history. Much of this can now be accomplished through security credentials issued by the Department. A real-time service would permit institutional applications to be aware, in real-time, of the NSLDS data can modify awards consistent with changes in the data. This would be done using an API. These applications could include a status report available to the student, again in real-time.

Dual Enrollment

Dual Enrollment defined as a student enrolling in both a high school course and a college course at the same time. This requires coordination between the high school and the college depending upon state and district policies. As the number of these students increase, it will be important to have real-time data exchange on status, progress, and, in some cases, attendance (for state accounting purposes).

Concurrent Enrollment

Concurrent enrollment can be defined enrollment in two colleges and universities at the same time. Several years ago that rate was about 30%--it is increasing, especially in community colleges, as course availability is being reduced giving a student an incentive to take the course where available.

It becomes important since a student’s federal and state financial aid eligibility is based on the study at both institutions. Current regulations require that one financial aid officer take responsibility. However focus groups show financial aid officers are hesitant to provide that service since their college or university becomes responsible for a student on whom they may not have any information about enrollment until the end of the term (often via the PESC transcript from the second college or university).
Estimates suggest that 250,000 students enrolled in the California Community Colleges would be eligible for or for additional financial aid if these data could be exchanged immediately, consistently, and accurately.

Exchanges between K-12 and Higher Education

The Postsecondary Education Standards Council has developed two specifications for high school and college transcripts. A minimal choreography for request and acknowledgement has followed.

Real-time access to a PESC high school transcript from a SIFA-compliant student system will be possible though the details of the data transport between a SIF ZIS Zone Integration Server) and a college or university. (This delay responds to an informal request the specification not be completed until there was additional time for higher education to participate).

SIFA is also developing a student record specifically for providing a receiving teacher with the data that could be used by a teacher to better meets the needs of a student who transfers into the school. Colleges and universities may find these data useful, especially for students entering directly from a high school or participating in dual high school-college enrollment. This will extend the SIFA messages, but uses the data transport infrastructure is included in the 2.5 specification.

Exchanges Between Foreign and Domestic Colleges and Universities

PESC Board Member David Moldoff has represented PESC as an Advisor to the Steering Committee. There has been continuous exchange between the PESC/RS3G, JISC CETIS, and the ISO Committees for the past several years. The Bologna processes are sharply different from the U.S. because student mobility among universities depends upon recommendations from the sending university and acceptance and subsequent progress report of the student who is taking courses at another university. Credit is determined before a student “transfers” rather than after.

When U.S. students attend short courses taught by U.S. faculty at U.S. branches, data exchanges are not required. Data exchange is required for U.S. students that enroll in non-U.S. universities. However there is no standard electronic process; exchanges of paper and facsimile forms are typically used. The National Association of Foreign Student Advisors (NAFSA) participated in the early discussions between PESC and RS3G representatives participating in the PESC Summits.

This data exchange will likely follow the RS3G process, data models, and protocols because of the early and broad implementation. However, collaboration between PESC and RS3G will improve integration.

Joint Information Systems Committee (JISC) research has described an exchange of course description data among universities and with UCAS (Universities and Colleges Admissions Service). This parallels a similar PESC project. The PESC project has fewer data elements.
It is likely this will be adopted for other European Higher Education Area colleges and universities replacing paper and Website documentation.
Appendix 4a, a day in the life of Ralph Registrar

A major University in the northeast  Ralph Registrar, the University Registrar

12:20am

Working with the campus emergency management team, Ralph just concluded that the impending winter storm would result in closing the campus and canceling classes. The University Provost has instructed Ralph to notify all students, faculty, and staff of this decision. Classes begin at 8:00 am.

12:25am

Using a SAML protected web application, Ralph uses his campus issued credentials to verify that he is the Registrar, and sends a campus closure message to all students, faculty, and staff using the campus emergency management communication system. This results in automatic updates to: multiple campus Web sites; local TV/radio and campus newspaper; text or email message to all individuals; starting at 6:30 am automated phone updates to all individuals that have elected to receive.

12:35am

Today is the campus-wide day of early-semester exams. Ralph notifies the campus scheduling office to reschedule the exams for tomorrow. Exams will take priority over other events scheduled for tomorrow. Ralph is getting a headache and decides it is time to get some sleep.

6:30am

Ralph receives his automated phone notification and wishes he had not opted-in to this service.

7:30am

During last nights' conference call, the Provost informed the enrollment management team that the 8:30am meeting will be held as scheduled. The fall enrollment decisions need to be finalized today - storm or no storm. Ralph logs into the executive information system, again using his campus issued credentials, and extracts current data regarding fall admission and spring enrollment. Because he is already logged in this morning, he is able to update the enrollment management model via the portal.

8:30am

Ralph presents this current forecast of fall admission. Without logging in again, he is able to transfer this current data into the campus financial aid model and final admission criteria are established.

10:00am

In the office with little support staff (the campus is closed) Ralph receives an emergency call from an upset parent; she has not talked to his son for 3 days. The parent used her University issued credentials to access the sections of the student information system she was entitled to, and discovered that she was no longer able to view information that she previously had access to. The parent is thinking her son has run away and is asking Ralph for information about her son's academic record and performance in class. Ralph opens the student information system, where is already established credentials are able to grant him access, and learns that the son has placed a no-information-release on his record (which also blocked his mother's access) and also sees that
the student withdrew last week. Ralph's headache is returning, but at least the system is working as designed.

11:00am

Without any further authentication, Ralph opens the employee database to extract information on his employees that are due to receive their annual performance evaluation within the next 45 days.

Noon

Using the portal and his previously acquired credentials, Ralph verifies the results from the campus scheduling office regarding tomorrow's rescheduling of exams and other events. Because his credentials prove that he is the Registrar, he is able to approve the plan. While on the site, he learns that the special seminar for the class he is teaching needs to be cancelled.

12:45pm

Because his special seminar needs to be cancelled, Ralph moves to the campus course management application, and informs his students. Since the seminar cannot be rescheduled, Ralph updates the course syllabus to provide an alternate assignment. This requires a change to required textbooks; Ralph notifies the campus bookstore to allow a full refund for returned textbooks from his students.

1:30pm

The snow stops!

3:00pm

Having responding to all of his daily email, Ralph decides to leave the (closed) campus and go home. The snowplows have cleared the parking lot and have successfully plowed in Ralph's car. Using his smart phone, he uses a campus provided web app to contact the emergency services department. Providing his executive authentication information on first login invokes prompt and free-of-charge assistance with his auto.

3:20pm

Ralph is on his way home and receives an emergency text message from the President. The President is traveling tomorrow on a fund raising trip and needs information on the number of University alumni in the city he will be speaking. Being a "text-free" driver, Ralph pulls his car into a parking lot and uses his smart phone to connect to the campus data warehouse to obtain the information for the President. Since he just used his smart phone to log into the emergency services department, he need not do so again, since the data warehouse is also SAML protected. Ralph transfers the requested data to the President via the secure data server so the President may access.

4:10pm

Ralph arrives home safely and begins clearing his driveway and sidewalk.

5:50pm

With the outside work complete, Ralph turns on the local evening news. A new storm is on the way. Ralph's headache is back.
Appendix 4b, Student Stories

**Community College Student:** I started out at a local community college because I was not accepted by the four-year college I wanted to attend. I knew that I could do better than what my record showed so far. I planned to follow the outline of a transfer agreement my community college had with a four-year university and earn my associates degree in business marketing, which would guarantee my admission later on down the road. Now I am in a completely different place than I originally intended. I did not end up at the four-year I first wanted, rather I am Journalism major at a smaller, private university. After spending two years at a small community college, I was no longer interested in going to school with a lot more students and a huge campus. I no longer was able to rely on the transfer agreement between my community college, so I knew that trying to find a smaller school that would accept my transfer credits would be a problem. It took a lot of research and time, but I finally found a school that offered what I wanted and that would accept most of my courses for transfer. I still lost a semester of credits. I frequently wanted to just hang it up and go to the big school because it was easier to get admitted and I knew all of my courses would transfer, I decided that I had to put in the extra effort to go to a school that would be a better fit for me if I wanted to be successful.

**Community College Student, with Federated Authentication:** When I proved my identity to take my SAT test, I was given a username and password that gave me access to a set of credentials that any college or university in the country will accept. When I wasn't accepted to my school of choice, I enrolled in the local community college, fully intending to take advantage of their transfer agreement with the state university. But, that was not how things worked out. After I decided to investigate other alternatives that would better suit my needs, I was able to log in using those credentials I had been issued at the beginning of my college career and start doing some real research. I discovered that colleges and universities had taken the effort to document course descriptions, so when I started asking colleges what they offered I was able to quickly see courses that might be of interest to me, and they were able to quickly evaluate the detailed descriptions of the coursework I had already completed. Yes, I did lose nearly a semester's worth of work, but I know for certain that I am attending the school that best meets my needs, and I have received the maximum amount of credit for my prior work. It was easy to discover what I needed to know, universities work together to provide excellent service, and I can view every university's information with a single log in. I think that the universities win, too, because as they share course descriptions they are able to recruit students who really know what they want and where to get it, and as they are able to quickly evaluate a student's prior effort they are able to compete with other schools to offer potential students an accurate assessment of what they can get credit for.
Small Liberal Arts College: After two years at a small liberal arts college, I decided that the social life was lacking and it was time for a change. After setting my sights on a larger more urban public college I began to look into what, if any, of my credits they would accept for transfer. The process was very convoluted. My first choice was not interested in me, and more specifically they were not interested in accepting my courses for transfer credit. So, I started over with a new school in mind. And, I started over and over and over…and then I lost count. With each new attempt I had to start from scratch, and much of what I really needed to know was hidden from my view because I did not have the correct access to see it online, so I ended up on the telephone for hours. It would have been so nice to be able to select my transcripts from my college’s system and just move them to all the schools I was contemplating enrolling at all at once. I finally found a school that was willing to give my transfer credits and me a chance.

Small Liberal Arts College, with Federated Authentication: Because my small liberal arts college is a member of the InCommon Federation, I am able to use my college log in credentials to access not only my college's systems, but certain systems at other schools in InCommon. When I decided to leave my small school for a larger urban public college, I was able to log into my schools' transcript system using my credentials, and select 14 different larger schools all over the country to submit my transcripts and a preliminary application to. Within hours I began to receive emails from counselors at these schools, letting me know which of my credits would transfer, and which wouldn’t, and why. They were able to do so because the courses were well described in my college’s catalogue using PESC approved standardized vocabulary, so it was easy for them to use their systems and credentials to quickly review the course descriptions for my work and compare them to what their school offers. So, because all these schools belong to InCommon, and subscribe to standards promoted by PESC, they are able to rapidly get permission to access all the information they needed to make informed decisions about my requests. The last responses came back to me within 3 days of my mass request for information, and now I have what I need to formally apply to the schools that are the best fit for me. I will do this using my credentials from my existing school to identity who I am, saving multiple steps in the application process. Instead of spending untold hours on the phone, I was able to discover the schools that are best for me and interact with them quickly and efficiently. The schools I dealt with were confident that I am who I claim to be based upon my having proved my identity once when I first enrolled at my current school. The outcome could not have been better.
Military learner: While I was serving in the Navy, I took several training courses to improve my knowledge and skills as an aircraft mechanic. After boot camp I was initially stationed in Norfolk, then transferred to South Carolina, and finally Georgia. I took several CLEP tests while my ship was stuck in a shipyard in Naples, Italy. While aboard ship I also took distance-learning classes, and on shore duty in Georgia I attended college classes, both through the Navy Servicemembers Opportunity Colleges program. I eventually left the service and had to figure out how to finish college with records spread across multiple institutions by enrolling in a yet a new school. I had to request transcripts from each institution as well as my academic records from the Navy, since some of the training courses I completed over my Navy career were offered as equivalent to college credit. I had to contact each institution directly to get my course transcripts. In some cases I had to use the phone and rely on the US Mail. Other times I was able to do the work online, but only after I went through various procedures to obtain a username and password. It was a challenge proving I was who I said I was! It took six months to collect my transcripts and provide them to my chosen schools for validation. This work has gone a long way to helping me get my degree, but it is a very slow and arduous process bridging the institutions, the Navy and American Council on Education (ACE). When I enrolled, I received college transfer credit by having my college courses and military experience recommended by ACE, but all my Navy training records had to be forwarded to them to make it happen. Now I am working on earning my bachelors degree in Emergency Medical Service Management through another school that offers distance learning opportunities, but the path was so challenging that I nearly gave up on it several times.

Military learner, with Federation: When I took my first CLEP test, I used my military ID card to prove my identity to the proctor. They took down the information from my military ID and entered me into a server hosted by the College Board. I had no idea at the time how powerful this was going to prove to be. Every time I took a new CLEP test is used the username and password that I received with my first test score to prove my identity. When I got out of the military I asked about my college benefits during my exit interview. I was told that I could use that same username and password that I was issued by the College Board to enter the world of higher education. I chose a dozen potential schools that I thought I might be interested in. I visited the Common Application web portal, where I was able to use my College Board credentials to log in and select all the schools I have attended and all the schools I wanted to consider me. My transcripts were transferred automatically, and an admissions officer at each school was able to assess my suitability for their school and make an offer to me if they were interested. Within weeks I had several firm offers from great schools to choose from, detailing how much it would cost and how much credit I would receive for all my prior effort. What a breeze, I wish classes were as easy as getting in was.
A Bedtime Story for Student Services

It's 3:00 am and Bianca is sitting in a 24 hour Starbucks in the spring semester of her senior year, working on her Physics 456 homework. In a browser, she clicks on the link to the course management system, logs in with her University web single sign-on userid and password, and starts viewing the course information.

Next, she clicks on the homework link hosted by a third-party provider and "Welcome Bianca" appears along with her new homework assignment for that class. After finishing that, she decides to check her loan status and surfs to the web site of her financing agent. She clicks "Access your record" and is presented with an aggregation of her loan liability without having to identify herself or login.

She takes a deep breath, wondering if any of those job applications had yielded an interview. She clicks on her shortcut to the job placement service and again is presented with the status of her applications, without having to identify herself. One company is requesting an interview, so Bianca purchases a cheap airline ticket offered by an online service that sells only to students. In the past, she had to provide proof of enrollment, but now the technology handles this in the background.

Bianca occasionally wonders what the institution is giving out to other service providers like the financial aid, job placement, and other companies on her behalf. She cares about her information and doesn't like her address and cell number available. She decides to check how this is done and clicks on the "Control your information" link provided on the web single sign-on page. She is presented with the campus information release policy that includes the policy and specific information about online transactions. Bianca knows that each of the transactions she has completed tonight implied that the institution was passing identity information on her behalf to the other sites so they could authorize her to access her information there. She opens the list of sites that she has visited and reviews the type of information that is sent. No, that all looks okay to me. She notices that there's a music site that her institution has an agreement with, but she doesn't use. She clicks the "do not pass information" box, knowing she now can't access the service, but that they won't know anything about her either.

In April, Bianca graduated. One day she was a student and the next, an alumna. She noticed her access changed too. She now could get to an alumni networking service where she put out a query about apartments in the Bay Area. Her loan status had changed on the financing agent's site. She now was out in the wide world of opportunity and responsibility.

---

12 https://spaces.internet2.edu/display/InCCollaborate/A+Bedtime+Story+for+Student+Services
Appendix 5, Data Exchange with U.S. Federal Government Departments and Agencies

Data exchanges with the U.S. Federal Government require compliance with federal law, regulations and practices. The practices and interpretations are emerging. This bibliography lists documents relevant to those discussions.

According to a briefing of software developers, the U.S. Department of Education’s Federal Student Assistance student data would require a NIST Level of Assurance 2.

In addition to these documents, the guidelines published by the National Institute of Standards and Technology (NIST) in these Special Publication series applies. OASIS security specifications are being implemented by schools, colleges and universities and should be consulted as well.


