



The Identity Management Collaborative: Remote Middleware Support



NMI-EDIT Case Study Series

In response to calls from the higher-education community, the NMI-EDIT Consortium has developed a series of Identity Management Case Studies to explore the planning and implementation of this critical infrastructure at higher-education institutions around the country.

In the Spring of 2004, NMI-EDIT released the Extending the Reach Call for Proposal with the overall vision of exploring possible models for middleware support and informing the NMI-EDIT outreach and development efforts through collaboration with a wider, more diverse group of institutions. The work outlined in this case study was supported in part by the NMI-EDIT Extending the Reach Program.

This NMI-EDIT Case Study Series is sponsored by the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium of EDUCAUSE, Internet2, and SURA. Additional support was provided by the National Science Foundation Cooperative Agreement NSF 02-028, ANI-0123937. Thanks are extended to the authors: Mark Crase, Dan Malone, Maithreyi Manoharan, and Theresa May

Copyright © 2006 by the California State University. All rights reserved.



Executive Summary

The California State University (CSU) has undertaken a middleware development project intended to result in the creation of a system-wide Identity and Access Management Infrastructure. The Identity Management Collaborative (IdMC), begun in July 2004, is an identity management pilot project intended to help the CSU learn how to leverage the technological and intellectual resources across the CSU System in such a way as to avoid the need for deploying unique, stand-alone middleware solutions at each campus.

The IdMC was managed by the CSU Office of the Chancellor under an Extending the Reach (ETR) grant from the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium and included the California Polytechnic State University (Cal Poly) in San Luis Obispo, which played the role of service provider for enterprise directory and enhanced authentication services to the client campus, California State University Stanislaus. In addition to deploying reliable and effective services to the client campus, project deliverables included the development of a

client campus needs assessment model, as well as scope of work and project plan templates.

The IdMC succeeded in achieving all of the desired outcomes – Cal Poly provided the required services and support to Stanislaus and all other deliverables were provided. The benefits of the project were numerous and included:

- Provision of remotely supported identity management and access services at Stanislaus using fewer financial and personnel resources than would have been required had Stanislaus implemented the services locally.
- Enhanced technical expertise and improved systems at the Cal Poly campus.

Lessons learned included:

- Validation that multi-campus efforts can result in improved service at reduced development costs.
- Success was dependent on clearly defined priorities, strong project coordination and management, and assistance with start-up funding.

NMI-EDIT Components Highlighted in this Case Study

eduPerson Directory Schema

eduPerson contains identity-related attributes for higher-education institutions for deployment locally and to foster inter-institutional collaborations.

<http://www.educause.edu/eduperson>



Enterprise Directory Implementation Roadmap

<http://www.nmi-edit.org/roadmap/directories.html>

The Enterprise Directory Implementation Roadmap is a web-based collection of resources that institutions can draw on to help deploy and use enterprise directories in higher education and research communities.

Web Initial Sign-On (WebISO)

<http://middleware.internet2.edu/webiso/>

The WebISO Working Group is investigating the realm of "web initial sign-on" (WebISO) packages designed to allow users to authenticate to web-based services using a standard, central authentication service.

Local Domain Person Object Class Study

<http://middleware.internet2.edu/dir/>

In the fall of 2003, a survey was circulated via Internet2 and EDUCAUSE email lists to determine how institutions are using locally-defined person object classes or attributes in their enterprise LDAP directories. This document is an analysis of the results provided by 23 institutions as of April 20, 2004.

LDAP Recipe

<http://middleware.internet2.edu/dir/>

This document is intended to be a discussion point toward the development of common directory deployments within the Higher Education community.



The Identity Management Collaborative: Remote Middleware Support

In July 2004, the California State University (CSU) began a middleware development project intended to result in the creation of a system-wide Identity and Access Management Infrastructure. The CSU serves more than 400,000 students through the efforts of 44,000 faculty, staff and administrators across 23 campuses. The goal of the Identity Management Collaborative (IdMC) is to learn how to leverage the technological and intellectual resources across the CSU in such a way as to avoid the need for deploying unique, stand-alone middleware solutions at each campus.

Within this context, one of CSU's objectives is to create mechanisms whereby campuses with the capability can provide identity management services to campuses with more limited resources.

The IdMC served as a pilot project for the broader identity and access management initiative and helped the CSU identify the costs, benefits and challenges related to providing middleware support services remotely. The IdMC used a small-scale service model whereby the Cal Poly San Luis Obispo campus supported the CSU Stanislaus campus by delivering directory and basic authentication and authorization services for a defined set of applications and related users.

The Business Problem

A successful collaboration can occur only when the collaborators have a shared set of goals that serve the business needs that are distinct to each organization. In the case of the IdMC, the Office of the Chancellor, CSU Stanislaus and Cal Poly San Luis Obispo shared the desire to improve identity and access management standards and practices in the CSU, but they also had unique business challenges that needed to be addressed in the project.

Office of the Chancellor

From the perspective of the Office of the Chancellor, the key business problem was finding a way to establish identity management services at a campus with limited personnel and financial resources. Additionally, it was desirable to create a collaborative model for developing and supporting these services that could be exported to other campuses with similar resource constraints.

Stanislaus

With the increased number of existing applications (e.g., Banner, Blackboard, email, PeopleSoft) that require login identifiers and passwords for faculty, staff and students, and with new applications being added constantly, it became obvious that the Stanislaus campus needed an infrastructure for helping the campus



community manage access to these applications. Additionally, the need for a single point of control for managing authorization to services had become a necessity.

The original solution was to start with a portal, but it quickly became obvious that to achieve the desired single sign-on (SSO) functionality, it was necessary to start with an Enterprise Directory. Therefore, the initial scope of the project was expanded to include building the Enterprise Directory System (EDS) and to enable SSO through the Oracle Portal for general access to email, Banner and Blackboard, and for administrator access to PeopleSoft HR 8.0.

The major stumbling block to planning and implementing an EDS and any related authentication or authorization services, was a serious lack of campus resources. The Central IT budget had been cut 24% in the last two years, resulting in very low levels of staff and equipment resources, as well as reduced funding for training staff to implement an EDS infrastructure.

Joining the Chancellor's office and Cal Poly San Luis Obispo in the IdMC project represented a solution to the problem and prompted the Stanislaus campus to join the project.

San Luis Obispo

In contrast to Stanislaus, the San Luis Obispo campus began implementing an identity and access management

infrastructure in the summer of 2002. During the past three years, Cal Poly has enhanced its infrastructure by establishing an LDAP-compliant enterprise directory within a high availability environment, a Central Authentication Service (CAS)¹, a robust identity reconciliation system, and an account provisioning model for the campus. However, there is a constant need to enhance the service, improve the reliability of current tools, and to evaluate new identity management technologies to determine their fit with the campus' infrastructure.

When Cal Poly was approached to participate in the IdMC, it was clear to the project team that San Luis Obispo could gain much from the collaboration. By becoming a Service Provider (SP) for CSU Stanislaus, San Luis Obispo would benefit from an outsider's perspective of the Cal Poly service, gain knowledge from colleagues at other campuses, and receive feedback regarding the effectiveness of the processes, software and tools being used at Cal Poly. Additionally, collaboration on identity management would generate crossover benefits in other areas. For example, both San Luis Obispo and Stanislaus were implementing the Oracle Collaboration Suite, and interaction in the identity management domain could lead to knowledge sharing with respect to implementing other Oracle tools.

¹ For more information about CAS, see: <http://www.ja-sig.org/wiki/display/CAS/Home>



The Cal Poly team also saw the IdMC as a way to improve campus-focused services. The project would allow the campus to enhance the local infrastructure, review and improve related identity management policies and procedures, add services, enhance user support, and achieve greater efficiencies through economies of scale.

IdMC Goals, Objectives and Deliverables

Office of the Chancellor

The primary goal of the IdMC from the Chancellors Office perspective was to foster the development of identity and access management standards and practices in the CSU. It was also critical to understand what challenges and benefits, if any, there were to developing a multi-campus identity and access management support model. The Office's objectives for the IdMC were to:

- Define a process for identifying the identity management needs at any given campus.
- Develop a template for defining a specific campus' business case for identity management.
- Develop a template for a service agreement that would be used when one campus assists another on providing identity management services.

Stanislaus

From the perspective of the Stanislaus team, the overarching goal of the project was to provide basic directory and

authentication services to the campus community. Specific objectives included:

- Authenticating as many applications as possible using the Enterprise Directory:
 - Formalizing procedures for adding applications. In addition to the initial Oracle Portal, email, Banner, Blackboard and PeopleSoft HR 8.0 applications, the campus will eventually enable access to Help Desk, Imaging, and One-Card applications, as well as Active Directory in labs, Library and Wireless Access.
 - Creating procedures to include authentication functionality when new applications are being planned.
 - Developing a knowledge base for both the campus community and vendors regarding authentication procedures for Stanislaus.
- Development of a plan to host the directory locally within three years. The plan needed to include a feasibility study to identify needed resources and also had to identify migration strategies.

Within the IdMC, Stanislaus was responsible for the following:

- Creating a secure method of transferring data to San Luis Obispo in order to populate and maintain the Enterprise Directory.
- Identification of the types of data (public vs. non-public).



- Identifying people from Stanislaus who would be updating information in the directory.
- Creating a campus communications plan.
- Documentation of any required policy statements or agreements, especially those dealing with data access and authorization.
- Creating a knowledgebase of frequently asked questions (FAQ) about the directory and authentication services.
- Training pilot groups in the use of the portal, SSO procedures, and any related applications.

San Luis Obispo

Since San Luis Obispo already had a well-established identity and access management infrastructure, the Cal Poly team had a different set of goals and objectives, which were:

- To enhance the campus' existing Identity Management Infrastructure by:
 - Upgrading software to newer versions (Oracle Internet2 Directory 10g and CAS 2.012).
 - Implementing LDAP replication.
 - Implementing CalStateEduPerson and NMI-EDIT's [eduPerson²](#) directory schema.
 - Enhancing technical and procedural documentation.
- Enhancing cross-campus collaboration by facilitating sharing between campuses.

For its part, San Luis Obispo was required to:

- Provide a formal scope of work to Stanislaus.
- Define security and reliability performance metrics related to the transmission and storage of directory information.
- Build and populate an LDAP-compliant EDS for use by Stanislaus.
- Enable CAS authentication services.
- Provide remote support for enterprise directory and authentication services with guaranteed availability of services 8:00 – 5:00, M – F for the pilot project.
- Define a migration strategy to a high availability (24x7x365) production directory.
- Integrate the Blackboard, Oracle Portal, and PeopleSoft HR 8.0 applications with the SSO process.
- Define a plan to move the pilot project into a production environment.

Implementation

From its inception in July 2004, the IdMC pilot was expected to run for one year and if successful, evolve into a long-term production service provided to Stanislaus by San Luis Obispo. Successful implementation of the IdMC depended on the coordinated efforts of three entities – the CSU Office of the Chancellor, Stanislaus, and San Luis Obispo.

Office of the Chancellor

The initial steps in developing the project were focused on establishing the project

² The [eduPerson Schema](http://www.educause.edu/eduperson) is located at <http://www.educause.edu/eduperson>

team, articulating the desired outcomes, identifying the needs of the collaborators, and defining the roles of the campuses and Chancellor's Office. A Project Oversight Group was created and charged with developing a detailed project plan and guiding project activities. The oversight group was comprised of the Senior Director, Technology Infrastructure Services from the Chancellors Office, and the Chief Information Officer (CIO) and technology management staff from each campus.

The first step for the IdMC project team was to conduct an identity management needs assessment for the Stanislaus campus. This was intended to help the team understand what Stanislaus needed to accomplish, and to help identify the specific project elements (business drivers, resource inputs, processes and products) required to meet those needs. Once the needs assessment was complete, the next step was for the Cal Poly team to develop a Scope of Work (SOW) to provide the services required to meet Stanislaus' needs. The SOW outlined specific service activities, costs and deliverables, and defined the roles the Cal Poly and Stanislaus teams would play in ensuring services would be provided on time and on budget. Finally, the SOW was used to develop Memoranda of Understanding (MOU) between the campuses and the Office of the Chancellor. The MOU document formalized the roles and responsibilities of the three parties and governed the related financial relationships.

Stanislaus

As the client, Stanislaus hosted the project kick-off meeting as well as the closeout meeting that marked the end of the pilot project. The campus team also participated in bi-weekly project status conference calls, in addition to periodic videoconferences and technical planning and implementation sessions.

With respect to implementation, the Stanislaus team was responsible for articulating its needs to Cal Poly, and for all of the activities related to developing the local business case for investing in identity management and communicating that case on campus - in particular, the CIO and project team had to develop a communications strategy and sell the value proposition of the IdMC to the campus community. This required the CIO to make presentations to the President's Cabinet and IT advisory groups, as well as to the campus faculty senate executive committee.

Operationally speaking, Stanislaus also had a significant amount of responsibility. They created the IdMC project web site, managed the project listserv, developed an identity management FAQ, and recruited and trained a subset of the campus community to serve as pilot user group. Furthermore, the Stanislaus team was required to help architect the directory structure and implementation process. This involved making decisions about identity reconciliation, provisioning, web login, and password management. They were also



responsible for designing the interface for CAS, and preparing and transmitting metadata to Cal Poly. In addition, Stanislaus needed to define local business rules that would guide use of the directory service, and then define password requirements, and create and distribute new passwords to the pilot group.

San Luis Obispo

As the service provider, Cal Poly hosted the initial technical planning meeting, and participated in all of the bi-weekly status update conference calls and videoconferences. In this capacity, they were also responsible for leading the Stanislaus staff through the directory architecture and development process by facilitating a number of technical planning meetings and by serving as a technical resource to the Stanislaus staff as they worked through various operational challenges. Cal Poly also developed the detailed project plan and provided periodic updates with respect to tasks, timelines and milestones.

Operationally, the San Luis Obispo team led the development of the directory architecture and defined the technical requirements for the identity management services being provided. Specifically, Cal Poly installed and configured the Oracle Internet Directory product, configured the related data warehouse, received the metadata from Stanislaus and populated the directory (see Fig. 1). Once the basic directory service was established, Cal Poly configured CAS and

provided web-based authentication services to the identified Stanislaus applications.

Benefits and Lessons Learned

Similar to the variety of motivations that participants had for joining the IdMC, the benefits they derived from their participation, and the lessons they learned along the way, varied as well.

Office of the Chancellor

The benefits to the Chancellor's Office for its participation were primarily related to being able to create a testbed environment for multi-campus collaborations in identity management. While members of the CSU professional community are often willing to work with colleagues at other campuses, there can be significant barriers to cross-campus collaboration. These include constrained financial resources, an uneven distribution of experienced staff, geographical separation and differing priorities across multiple campuses.

Participation in the IdMC benefited the Office of the Chancellor in two important ways. First, the Chancellors Office believes that multi-campus collaborations provide opportunities for improving services through the development of best practices, and can also lead to improved economies-of-scale in a time when resources are increasingly constrained. At least on this small scale, the IdMC validated this belief and will help inform larger-scale collaborations in the future. Second, it served as a testbed for



activities related to the CSU's system-wide identity and access management initiative by reinforcing a standardized approach to directory services that is based on the NMI-EDIT components in general, and the Cal State modifications to the [eduPerson](#) object

classification specifically. It is the intent of the CSU to adopt a standards-based methodology for directory services and the IdMC allowed the Office of the Chancellor to test the feasibility of such an approach.

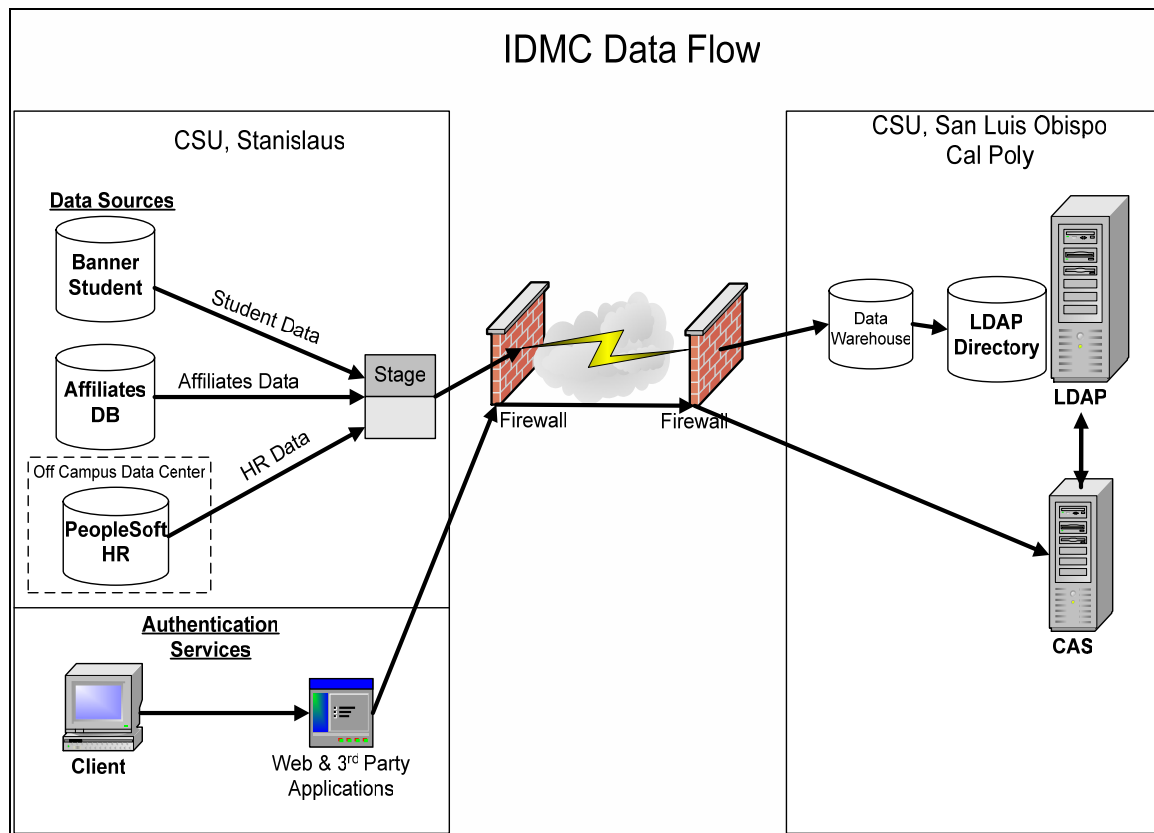


Fig. 1. The IdMC Data Flow from Stanislaus to Cal Poly. In this model, data is extracted nightly from the Banner Student, PeopleSoft HR, and Affiliates databases. This data is then stored in a series of staging tables. The connection between the Off-campus Data Center and the staging tables is established with an encrypted channel for data security. Next, Cal Poly extracts this data from the Stanislaus staging tables, and imports it into a Data Warehouse at Cal Poly. The data transfer from Stanislaus to Cal Poly passes through both campus firewalls, and the communication channels are encrypted to ensure data security. Once the data is in the Data Warehouse at Cal Poly, it is compared to the previous version of the LDAP data. A process then goes through a series of routines and creates the latest version of the LDAP directory that then replaces the current LDAP directory.

This model also demonstrates how a web application or third party application utilizes CAS authentication. The web application resides at Stanislaus, but during the authentication process, the application is redirected to the CAS server located at Cal Poly to provide the authentication services. Once authenticated by the CAS server, the user is redirected back to the originating application at Stanislaus.



The IdMC also provided valuable insights into how the potential for success of future collaborations can be maximized. Not surprisingly, sufficient financial support was determined to be a significant enabler. This support took two forms. First, the NMI-EDIT ETR grant helped offset the cost of staff assigned to the project and enabled their travel to meetings they might otherwise not have been able to attend. Second, moving the directory services into production mode required the purchase of additional server hardware that the Office of the Chancellor paid for as a one-time purchase. Together, these expenditures totaled less than \$75,000, and demonstrated that while financial support for such projects is critical, the investment required to catalyze the project was not dramatic.

Another valuable lesson gleaned from the IdMC was that while the collaboration would not prove beneficial without the efforts of the various campus participants, the project plan developed by Cal Poly, and the logistical support provided by the Chancellor's Office were critical to keeping the project focused and on track. The former delineated the tasks, sequences and dependencies necessary to complete the project. The latter, on the few occasions when local activities threatened to obscure the importance of the project, helped focus attention on the task at hand.

Stanislaus

The benefits that accrued to the Stanislaus campus were varied but fell into two broad

categories: improved services to the campus community, and enhanced operational expertise. Within the first category, Stanislaus gained an enterprise directory and improved authentication services, with a relatively modest financial investment and no increase in staffing. This in turn led to an immediate improvement of service to the campus through the provisioning of email and PeopleSoft HR services, which was to be followed shortly by improvements in provisioning access to the Blackboard learning management system.

Within the category of enhanced operational expertise, Stanislaus staff gained valuable first-hand experience with the NMI-EDIT components. With Cal Poly's assistance, Stanislaus was able to create many of the technical components required to support an enterprise directory, in particular:

- Developed identity and access business rules and policies.
- Gained exposure to LDAP directory concepts and issues, including determining needs, set-up, configuration, and operational requirements.
- Gained access to an LDAP directory that has a common interface to multiple applications and eliminates duplicate staff and student records.
- Applied the knowledge they'd gained by beginning the provisioning of email services.
- Took an important first step in being able to integrate and provision other applications.



- Took a first step towards implementing Oracle Collaboration Suite (OCS).

Additionally, participation in the IdMC proved to be a valuable learning process for the staff, and a valuable opportunity to share best practices in identity management. The collaboration was a learning experience for all involved, with the potential for serving as a model for other multi-campus collaborations.

Finally, an unanticipated, but very valuable benefit of Stanislaus' participation in the IdMC was heightened awareness on campus of the value of directory-enabled services. As the campus considered developing or upgrading other systems and applications, utilization of the enterprise directory became one of the first considerations in the development process. This mindset has made the development process more comprehensive, and it is anticipated that over time it will help reduce some of the complexity related to application integration.

The lessons learned at Stanislaus can largely be categorized by the statement, *"Regardless of whether or not you contract with others to provide your enterprise directory, there is still plenty of work to do"*.

Challenges remained with respect to:

- Obtaining buy-in from all constituents.
- Educating constituents on concepts related to remote directory services.
- Configuring and maintaining security and reliable access (e.g., multiple

firewalls, remote access, SSL, hardware and software updates).

- Allocating the staff time and resources required for project (in spite of the time and resource savings from collaboration).
- Integrating disparate applications.
- Overcoming technical obstacles (e.g., configuring secure communications channels between databases and campuses and through firewalls).
- Coordinating source data to assemble into one LDAP directory, including answering common questions such as, "Who owns the data?" and "What do we do with the duplicates?"
- Resolving conflicts with competing campus priorities. The time team members could devote to the project was often limited because of their regular assignments.
- Synchronizing and coordinating activities between two campuses. Often when one campus was able to spend time on the project, the collaborating campus was overwhelmed with other responsibilities.
- A lack of cooperation from software vendors in solving the project's integration needs (e.g., difficulty interfacing with certain proprietary or closed learning management systems).
- Finding software vendors offering reliable and usable products with the necessary features to implement an identity management system.



San Luis Obispo

The Cal Poly team also realized technical and operational benefits, but having already implemented a reliable identity management and access infrastructure at the San Luis Obispo campus, the team envisioned additional benefits that were somewhat different from those at Stanislaus. Cal Poly believed that they could improve local systems and services by refining their skills and processes as they helped their Stanislaus colleagues deploy an enterprise directory and authentication service. The local benefits of San Luis Obispo's participation in the IdMC included:

- Improved buy-in at the San Luis Obispo campus regarding identity management initiatives by describing the CSU sanctioned initiative, the CSU Stanislaus implementation effort, and the possibility of interacting with other campuses in the future.
- Gaining enhanced expertise in directory and authentication technologies by working on the Stanislaus project.
- Enabling SSL on the Enterprise Directory to support secure communication with the directory.
- Obtaining input from the CSU Stanislaus team regarding Cal Poly's implementation.
- Implementing the Oracle Internet Directory (OID) 10g R2 software.
- Implementing replication of directory data between two OID servers.
- Gaining experience with CAS 2.012.
- Implementing the [eduPerson](#) directory schema within the Enterprise Directory.

- Provisioning directory data from the Identity Management Infrastructure.

The lessons learned along the way at San Luis Obispo related primarily to determining how best to manage competing priorities. Specifically, Cal Poly had a number of local projects being implemented during the same time period as the collaboration effort, making the allocation of resources extremely difficult. It is important that other campuses considering providing services to a client campus realize that the resulting services are contractual obligations and must be considered a campus priority - even if the benefits accrue elsewhere.

More Information

For more information on The California State University's IdMC and remote middleware support activities, the following individuals may be contacted:

Mark Crase, Ed.D.
Senior Director, Technology Infrastructure Services
California State University Office of the Chancellor
mcrase@calstate.edu

Roland Johnson
Manager, Academic and Instructional Technology Support
California State University Stanislaus
rjohnson@csustan.edu

Dan Malone
Middleware Architect



Cal Poly San Luis Obispo
dmalone@calpoly.edu

Theresa May
Information Management Coordinator
Cal Poly San Luis Obispo
tmay@calpoly.edu

