



**Federated Identity Management Evaluation  
NSHE iNtegrate Project**

**Nevada System of Higher Education**

**May 20, 2010**

**CIBER, INC.  
1401 WILLOW PASS ROAD  
SUITE 800  
CONCORD, CA 94520  
(626) 827-6406**

## Table of Contents

Executive Summary .....	3
Federated Identity vs. Single Sign-On .....	5
Single Sign-On .....	5
Federated Identity .....	6
Summary of Requirements .....	7
Current Infrastructure and Technologies.....	8
Possible Solutions.....	9
Centralized Statewide Identity Provider .....	10
Federated Identity Provider.....	12
Centralized Identity with Institutional Identity Providers .....	15
Migration Process to a Centralized Identity .....	18
Create Centralized Identity only when Required .....	19
Migration Process to a Centralized Identity only when Required.....	22
InCommon .....	23
Summary .....	26
Appendix A – Resources Consulted .....	27
Appendix B - Oracle PeopleSoft Solutions.....	28
Appendix C - Arizona State University .....	29
Appendix D - California State University .....	30
Appendix E - University of Central Florida .....	31

## Executive Summary

---

The Nevada State System of Higher Education (NSHE) is in the process of implementing Oracle PeopleSoft Campus Solutions 9.0 as the new Student Information System for all institutions within the System. As part of this project, NSHE identified a requirement to provide a Universal ID, along with universal authorization and institution level provisioning for all users of the PeopleSoft application.

NSHE has adopted a hybrid model for its PeopleSoft Campus Solutions implementation, in which several institutions are sharing a single Campus Solutions instance, and other institutions, such as UNR, will have their own instance of Campus Solutions. An individual may have roles at several different institutions. For example, a student at TMCC may be an applicant at UNR, and may have taken classes at UNLV and CSN. In order to prevent duplicates, NSHE has implemented the Universal ID solution, and will create a single PeopleSoft ID (the EMPLID) for all individuals who need access to the system. Separate instances of PeopleSoft will be synchronized when an EMPLID is created or updated, so that duplicates are not created, and so that all instances have up to date information.

The vision held by the Student System Module Task Force includes the requirement that all NSHE students having a PeopleSoft EMPLID (now known as the NSHE ID) can access their student information in PeopleSoft (all instances) and can use the same NSHE ID to gain access to other institution specific (locally provisioned) student resources.

What are the alternatives for NSHE to develop a system-wide identity management/single sign-on solution that enables the vision of the Student System Module Task Force and preserves the investment in local authentication and provisioning solutions currently used at the institution level?

NSHE has asked CIBER to evaluate currently available solutions for authorization and provisioning. Based upon our discussions with NSHE staff, any solution NSHE implements will be:

- 1) Consistent with the principles outlined in the document, NSHE User Creation and Authentication.
- 2) Robust and secure so as to reduce long-term risk.
- 3) Easy and cost effective to maintain.
- 4) Flexible enough to accommodate those campuses with a solution already in place.
- 5) Cost justified.



## CIBER Higher Education Practice



This report will discuss the differences between Single Sign-On (SSO) and Federated ID (FID), give a high level summary of NSHE's requirements, and discuss several alternatives to provide both SSO and FID solutions.

## Federated Identity vs. Single Sign-On

---

The difference between Federated ID (FID) and Single Sign-On (SSO) is subtle. SSO unifies access management for disparate systems within an organization.

FID does the same, but across different organizations. In a sense, federated identity is SSO across institutional boundaries.

### ***Single Sign-On***

---

For an individual institution, under Single Sign-On (SSO), a user authenticates once to the local identity provider and has access to other applications at that institution without the need to re-authenticate when using each application.

A single sign on approach at an institutional level offers benefits to the majority of the student, faculty and staff population. Implementing SSO at an institutional level will reduce the identity maintenance required of the student, faculty and staff. The user population will need to manage one user name and one password for access to applications within the institution.

Currently, none of the NSHE institutions has implemented a SSO solution. The closest would be a single user name and password that is used across multiple applications, although this approach requires the user to re-authenticate with each application using the same credentials. In an SSO solution, the user would only authenticate once, to the first application.

Depending on the SSO solution (Tivoli, Oracle, Computer Associates (CA) or Shibboleth), each application needs to be configured (or modified) to accept the SSO token. Implementing an SSO package does not automatically give the institution a working SSO for their users, the applications must support the SSO package.

## ***Federated Identity***

A user authenticates to a local identity provider and is granted access to an external domain that accepts the local identity.

In a standard commercial FID solution, a stable user base is preferred. For example, company A outsourced its e-mail system to Google. Google will accept a federated identity from company A and allow the user access to their email. If the user moves to company B, their previous identity with company A to the Google email is lost. At company B, they will need to re-establish their federated identity with Google and have a new email or access the same if the email was personal.

If the analogy of company A and company B was applied to an institution such as UNLV and TMCC and Google was replaced by PeopleSoft; when a student moves between institutions, their privileges granted to their previous identity would be lost when a new identity is created at the new institution.

In an environment such as the Nevada System of Higher Education, students often move between the institutions within a geographical region, and even between regions, such as northern Nevada and southern Nevada. In such an environment, a student may have multiple active identities at the same time; one per institution. Each of these identities may have different privileges assigned. This creates significant administrative overhead for both the students and system administrators.

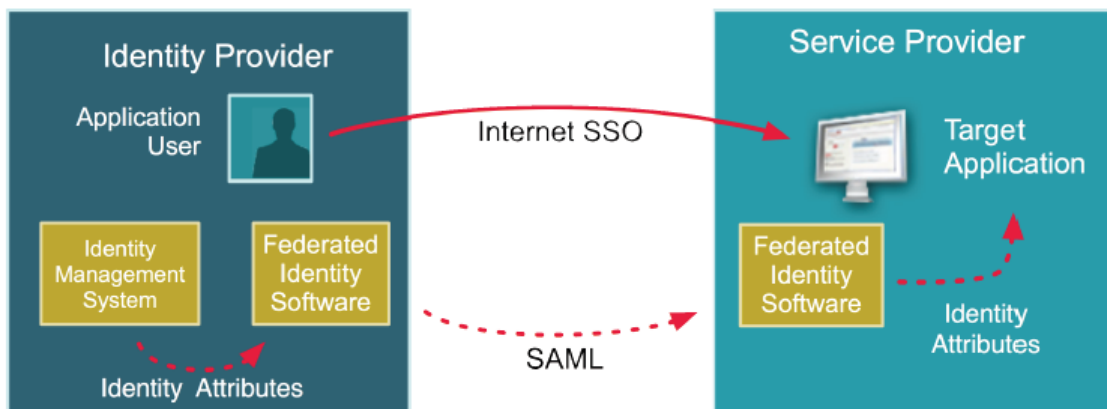


Figure 1 - From Ping Identity

## Summary of Requirements

---

The problem statement driving the requirements is:

*Can NSHE develop a system-wide identity management/single sign-on solution that enables the vision of the Student System Module Task Force and preserves the investment in local authentication and provisioning solutions currently used at the institution level?*

NSHE does not yet have a formal requirements document for this project. The high level requirements listed below have been compiled from the NSHE institutions and the staff of the SCS group through email surveys, individual interviews, and discussions with NSHE staff.

- Autonomy of institutions to select technology, infrastructure and set internal policies
- User names in each institution's directory services will be linked to the NSHE ID
- User names will be consistent across institutions. A user will only have to know one user name for all the institutions
- The user password will be consistent across institutions. A user will only have to remember one password for all the institutions
- Be able to synchronize a user's password across institutions
- Universal and consistent password policy for all the institutions
- Campus student portals will use the LDAP user name and password for authentication
- Wireless access authentication will use the LDAP user name and password
- Computer Lab access will use the LDAP username and password for authentication and authorization within the institution

## Current Infrastructure and Technologies

---

Institution	Directory Service	Faculty e-Mail	Student e-Mail	PeopleSoft Access	Student Username Standard
UNLV	Active Directory	Lotus Notes	Google	NSHE ID	SWAMI
UNR	Active Directory	Exchange	None	LDAP	<First Initial><Last Name> followed by conflict resolution algorithm
NSC	Active Directory	Exchange	None	TBD at implementation	SWAMI
CSN	Active Directory	Exchange	Ipswich IMail	TBD at implementation	"C" Number
GBC	Novell eDirectory	Group Wise	Google	TBD at implementation	SWAMI
TMCC	Active Directory	Group Wise	Google	LDAP	First_Last
WNC	Novell eDirectory	Lotus Notes	None	TBD at implementation	SWAMI

The current infrastructure and technologies have a common directory service, Active Directory (except for GBC and WNC). The majority of the faculty email is on Microsoft Exchange.

It appears that the direction for student email is either to eliminate institutionally provided email or outsource to Google. The only exception to this is CSN, which is currently maintaining an internal mail system for the students. Often there is a close relationship between the LDAP user id and the email id.

System-Wide Account Management Interface (SWAMI) is a legacy system used in the past to provision UNIX accounts, e-mail ids and HTML pages for students in the NSHE system.

The majority of student user names come from a centralized source, SWAMI or the "C"-number (which is the SIS ID, the legacy Student Information System). SWAMI ids are unique to every student in NSHE post 2002. The only exception to this is UNR and TMCC where they have implemented Active Directory user names for their students.











## Possible Solutions

In the following four sections, five possible solutions are reviewed. Each solution meets most of the requirements; however there is no one solution that meets all the requirements listed in the previous sections.

Each solution has a chart that maps its ability to meet a specific requirement. Each mapping is evaluated on a red, yellow green scale.

<b>Color Code</b>	<b>Description</b>
	Almost all of the requirement is met
	Some of the requirements are met
	None of the requirements are met

Each solution has a chart that maps its relative cost based on Implementation, Development, Migration and overall costs. Each mapping is evaluated on a red, yellow green scale.

<b>Color Code</b>	<b>Description</b>
	Lowest cost
	Medium cost
	Highest cost

## Centralized Statewide Identity Provider

---

With the statewide identity provider option there will be:

- Single identity provider for all institutions
- Statewide username base
  - Consistent username and password for all students, faculty and staff in all institutions
- One root domain with sub-trees for each institution

This is technically the most direct approach in achieving the goals and requirements stated earlier.

- One username and password per student, faculty or staff
- Same username and password will work at all institutions
- Provides global authentication across all institutions

However, this approach does not come without some drawbacks. This approach requires that all the institutions use the same directory service technology. Although six of the seven institutions (this does not include DRI) are using Active Directory, the one using eDirectory will need to migrate to an Active Directory structure. This will also cause problems for the institutions that already have an extensive Active Directory structure. These institutions (UNR and TMCC) will require a migration of their current environments into the new structure.

Requirements cross-reference:

Autonomy of institutions to select technology, infrastructure and set internal policies	●	There will be one NSHE level directory service. Each institution will be a part of this directory service. There will be a state-wide namespace for user names.
User names in each institution's directory services will be linked to the NSHE ID	○	The central directory service will be linked to the NSHE ID. Each institution will not have a directory service.
User names will be consistent across institutions. A user will only have to know one user name for all the institutions	●	By having one directory service across all institution, there will be only one user name and password per user in all institutions.

The user password will be consistent across institutions. A user will only have to remember one password for all the institutions	●	By having one directory service across all institution, there will be only one user name and password per user in all institutions.
Be able to synchronize a user's password across institutions	●	By having one directory service across all institution, there will be only one location that a user needs to change their password. The password change will affect every institution.
Universal and consistent password policy for all the institutions	●	By having one directory service across all institutions, there will only be one set of password policies.
Campus student portals will use the LDAP user name and password for authentication	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use the central LDAP server.
Wireless access authentication will use the LDAP user name and password	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use the central LDAP server.
Computer Lab access will use the LDAP username and password for authentication and authorization within the institution	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use the central LDAP server.

Costs:

Implementation Costs	●	May require additional hardware to support the Active Directory servers. Software costs already included in servers.
Development Costs	●	Minimal development costs. Will vary on the level of automation.
Migration Costs	●	Migration costs for existing Active Directory environments.
Total Costs	●	The migration costs of the existing Active Directory installation will far outweigh the low implementation and development costs.

## Federated Identity Provider

---

With the federated identity provider option there will be:

- Multiple identity providers; at least one per institution
- Each institution will need to install federation server software, such as ADFS v2 or Shibboleth
- Each institution will locally control the use of their resources and their user access (username and passwords)








This approach gives each institution the most autonomy on technology and infrastructure. Each institution may use any directory service; the institutions are not required to use a common technology. At each institution, each student, faculty or staff may have:

- A different user name
- A different password (unless the user co-ordinates their passwords manually)
- May have different password restrictions; depending on the password policy of each institution
- Will have different privileges granted to each user name from the external service provider (a federated service)

This approach is the least intrusive to the institution’s technology and infrastructure. It also accomplishes the least of the requirements listed above. This approach will still place the onus on the user population to manage their identities at each institution. However, it does simplify their access to the applications once the federation between each institution is established (at the application level).

Requirements cross-reference:

Autonomy of institutions to select technology, infrastructure and set internal policies	●	In a federated environment, each institution controls the technology, infrastructure and internal policies
User names in each institution’s directory services will be linked to the NSHE ID	●	This is an implementation choice, but can be mandated by NSHE

<p>User names will be consistent across institutions. A user will only have to know one user name for all the institutions</p>		<p>By having de-centralized directory services across all institutions, there could be a different user name in each institution for the same user.</p>
<p>The user password will be consistent across institutions. A user will only have to remember one password for all the institutions</p>		<p>By having de-centralized directory services across all institutions, there could be a different password in each institution for the same user.</p>
<p>Be able to synchronize a user's password across institutions</p>		<p>This could be done by changing the password based on the NSHE ID and each institution would have to accept the replicated password into their LDAP server.</p>
<p>Universal and consistent password policy for all the institutions</p>		<p>This can be accomplished by implementing the same policies in all the institutions. However, because of the de-centralization, it is not enforceable.</p>
<p>Campus student portals will use the LDAP user name and password for authentication</p>		<p>This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.</p>
<p>Wireless access authentication will use the LDAP user name and password</p>		<p>This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.</p>
<p>Computer Lab access will use the LDAP username and password for authentication and authorization within the institution</p>		<p>All computers within the institution will authenticate to the local LDAP server.</p>



Costs:

Implementation Costs	●	Will need software to support federated services. This could be minimal if open source products are used.
Development Costs	●	The applications that will be federated will need to be updated to accept the federated identity.
Migration Costs	●	No migration costs; as this does not alter existing infrastructure.
Total Costs	●	One time implementation costs are minimal. Development costs will decrease as development knowledge grows.

## Centralized Identity with Institutional Identity Providers

---

In the centralized identity with institutional identity providers model there will be:

- Centralized Identity management (directory service)
- Multiple identity providers; at least one per institution
- The user name is centrally controlled; similar to the NSHE ID
- Each campus will use the same user name created by the central directory service
- Central portal to replicate password to the identity providers at each institution
- Each institution will locally control the use of their resources and their user access

In this approach, each institution will maintain its autonomy on technology and infrastructure. The username namespace will be centralized to be statewide; this will guarantee a unique username within Nevada System of Higher Education.

Components to be built:

- Centralized Identity Management (could enhance SWAMI to meet the needs)
- Centralized user name and password policy
  - Password Complexity
  - Password Age
  - Password History
- Central portal to replicate password changes to each institution

Some non-technical issues:

- For replication of passwords to work, all institutions must agree on an encryption algorithm.
- Due to the statewide username namespace, migration will be an issue. There will be some user name conflicts between the eight institutions. A user name conflict policy will need to be developed.
- Users with user name conflicts will need special policies in the e-mail system to keep their previous email address with the new user id. For example, there is a conflict with user name **john**. His email address was [john@school.edu](mailto:john@school.edu). As a result of the user name conflict, his new user name is **john01**, but the user would like to keep his original email address. In Exchange 2007, his new primary email address would be [john01@school.edu](mailto:john01@school.edu), with a secondary address of [john@school.edu](mailto:john@school.edu). The primary email address is the address a recipient will see and reply to. Emails sent to the original address would still be routed to the new user. If this is not acceptable, then a custom mail policy can be created for the user so that their primary email address remains unchanged. This is an extra administrative step.

Requirements cross-reference:

Autonomy of institutions to select technology, infrastructure and set internal policies	●	In this environment, each institution controls the technology, infrastructure and internal policies
User names in each institution's directory services will be linked to the NSHE ID	●	This is an implementation choice, but can be mandated by NSHE
User names will be consistent across institutions. A user will only have to know one user name for all the institutions	●	The user name will be centrally controlled in a similar fashion as the NSHE ID.
The user password will be consistent across institutions. A user will only have to remember one password for all the institutions	●	By having de-centralized directory services across all institutions, there could be a different password in each institution for the same user.  This can be mitigated with the use of a central portal for the password changes.
Be able to synchronize a user's password across institutions	●	This would need to be developed. As stated above, the portal would be the password synchronization site for users.
Universal and consistent password policy for all the institutions	●	This would be a requirement as a result of the central portal for password changes. Every institution would have to implement the most restrictive policy among the institutions.
Campus student portals will use the LDAP user name and password for authentication	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.
Wireless access authentication will use the LDAP user name and password	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.





Computer Lab access will use the LDAP username and password for authentication and authorization within the institution	●	All computers within the institution will authenticate to the local LDAP server.
---	---	--

Costs:

Implementation Costs	●	Will need to create central directory service. Could utilize SWAMI and NSHE ID to support this. Need to agree on standards (see above).
Development Costs	●	Development of new portal site to support password changes and replication to institutions. SWAMI could also be updated to support this.
Migration Costs	●	User name conflict resolution will be manual. May also receive resistance to the new user name.
Total Costs	●	One time implementation costs are minimal. Development costs could be minimal if SWAMI is enhanced.



## ***Migration Process to a Centralized Identity***

---

To migrate to a centralized identity management system, all the current usernames in all institutions will be consolidated under one namespace. There are many ways to consolidate the usernames, institutions can be ranked by:

- Size of the institution (by user count)
- Complexity of current deployment
- Any other measurable criteria

Once the consolidation order has been determined, all the usernames from the highest ranking institution would be accepted into the directory verbatim. Then the usernames from the second ranking institution is added to the directory. If there is a conflict, the username will be altered according to a name collision algorithm.

This process would be repeated for every institution until all the users in all the institutions have been added to the central directory.

The name collision algorithm from UNR appears to be the most thorough, and should be used for the name collisions.

- First initial + last name
- Last initial + first name
- First initial + middle initial + last name
- First name + Last name
- First name + middle initial + last name
- First initial + last name + number (1-9999)



## ***Create Centralized Identity only when Required***

---

In order to reduce the user name conflicts, user name namespace could be left at the institutional level. A user will receive a centralized identity when they need to access multiple institutions. The centralized id may be n\_<old\_user\_name>.

In this scenario, users do not have access to other institutions by default. The access will be created when there is a need to access multiple institutions, and then the user name conflicts are resolved.

The process will be the same as above, but it will be limited only to the users that must access multiple institutions. The process flow is as follows:

1. PeopleSoft generates the EMPL\_ID (NSHE ID)
2. User is created in the local LDAP server of the institution A
3. User can use this id within the original institution to access applications and labs
- 4. User takes a course at institution B**
5. Institution B checks if the NSHE id exists in another institution. If it does, a request for a “centralized id” is made to the central directory service. The new user id generated from the central directory service would be n\_ prefixing a user name similar to the one in 2 (Institution A). Institution B would create this user in its local LDAP.
6. Institution A would be notified by the central directory to rename its user name for the NSHE ID to the one generated in step 5.
7. User can use this “centralized id” within Institution B to access applications and labs
8. User should be able to use the new “centralized id” at Institution A within 24 hours.
9. The user may now use the central portal to maintain their passwords. Changes from this site will be replicated to the two institutions
10. If this user takes a course at a third institution; during the user name generation process, the EMPL\_ID will be validated with the central directory to check if it has a central id. If it does, the central id name will be used.

Requirements cross-reference:

Autonomy of institutions to select technology, infrastructure and set internal policies	●	In this environment, each institution controls the technology, infrastructure and internal policies
User names in each institution's directory services will be linked to the NSHE ID	●	This is an implementation choice, but can be mandated by NSHE
User names will be consistent across institutions. A user will only have to know one user name for all the institutions	●	The user name will be centrally controlled in a similar fashion as the NSHE ID.
The user password will be consistent across institutions. A user will only have to remember one password for all the institutions	●	By having de-centralized directory services across all institutions, there could be a different password in each institution for the same user.  This can be mitigated with the use of a central portal for the password changes.
Be able to synchronize a user's password across institutions	●	This would need to be developed. As stated above, the portal would be the password synchronization site for users.
Universal and consistent password policy for all the institutions	●	This would be a requirement as a result of the central portal for password changes. Every institution would have to implement the most restrictive policy among the institutions.
Campus student portals will use the LDAP user name and password for authentication	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.
Wireless access authentication will use the LDAP user name and password	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.



Computer Lab access will use the LDAP username and password for authentication and authorization within the institution	●	All computers within the institution will authenticate to the local LDAP server.
---	---	--

Costs:

Implementation Costs	●	Will need to create central directory service. Could update SWAMI to support this. Need to agree on standards (see above)
Development Costs	●	Development of new portal site to support password changes and replication to institutions. SWAMI could also be updated to support this.
Migration Costs	●	User name conflict resolution will be only when a user requests a centralized id.
Total Costs	● ●	One time implementation costs are minimal. Development costs could be minimal if SWAMI is enhanced. Migration costs are per user per request vs. a mass migration

## ***Migration Process to a Centralized Identity only when Required***

---

To migrate to a centralized identity management system, all the users with access to multiple institutions will be consolidated under one namespace. There are many ways to consolidate the usernames, institutions can be ranked by:

- Size of the institution (by user count)
- Complexity of current deployment
- Any other measurable criteria

Once the consolidation order has been determined, all the usernames (with multiple institution access) from the highest ranking institution would be accepted into the directory with an “n\_” prefix. Then the usernames from the second ranking institution is added to the directory. If there is a conflict, the username will be altered according to a name collision algorithm.

This process would be repeated for every institution until all the users in all the institutions have been added to the central directory.

The name collision algorithm from UNR appears to be the most thorough, and should be used for the name collisions.

- First initial + last name
- Last initial + first name
- First initial + middle initial + last name
- First name + Last name
- First name + middle initial + last name
- First initial + last name + number (1-9999)



## 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.” See <http://www.incommonfederation.org/>

The members of the InCommon Federation are generally higher education institutions that are sharing local resources with other institutions. Typically, resources are research databases or computing resources. Other reasons for joining the InCommon Federation is to gain access to vendor applications such as Microsoft Live@edu, Apple and other library resources. See <http://www.incommonfederation.org/participants/> for a complete list.

Using InCommon to share student applications between Nevada institutions is very similar to the Federated Identity solution. To be a member of InCommon, each institution will also be required to:

- Meet InCommon security audits
- Pay an initial fee to join InCommon
- Pay a yearly fee to InCommon
- Install and configure Shibboleth

If a business case can be made for the InCommon Federation, it would be to support the faculty and staff. To take an InCommon approach to share student access to student application would be more expensive to implement than the Federated Identity solution because of the audits, initial fee and yearly fees. The software configuration is also dictated by the federation, everyone on it is using Shibboleth.

Requirements cross-reference:

Autonomy of institutions to select technology, infrastructure and set internal policies	●	In a federated environment, each institution controls the technology, infrastructure and internal policies
User names in each institution's directory services will be linked to the NSHE ID	●	This is an implementation choice, but can be mandated by NSHE
User names will be consistent across institutions. A user will only have to know one user name for all the institutions	●	By having de-centralized directory services across all institutions, there could be a different user name in each institution for the same user.
The user password will be consistent across institutions. A user will only have to remember one password for all the institutions	●	By having de-centralized directory services across all institutions, there could be a different password in each institution for the same user.
Be able to synchronize a user's password across institutions	●	This could be done by changing the password based on the NSHE ID and each institution would have to accept the replicated password into their LDAP server.
Universal and consistent password policy for all the institutions	●	This can be accomplished by implementing the same policies in all the institutions. However, because of the de-centralization, it is not enforceable.
Campus student portals will use the LDAP user name and password for authentication	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.





Wireless access authentication will use the LDAP user name and password	●	This is an implementation choice of the institution. This requirement can be met if the institution elects to use their LDAP server.
Computer Lab access will use the LDAP username and password for authentication and authorization within the institution	●	All computers within the institution will authenticate to the local LDAP server.

Costs:

Implementation Costs	●	Will need to install and configure Shibboleth software. This is often the issue with institutions joining the InCommon Federation. See article <a href="http://chronicle.com/article/Chasing-the-Single-Password/65343/">http://chronicle.com/article/Chasing-the-Single-Password/65343/</a>
Development Costs	●	The applications that will be federated will need to be updated to accept the federated identity.
Migration Costs	●	There will be migration costs for each institution to update security practices to meet the requirements of the federation.
Total Costs	●	The implementation costs of Shibboleth and security practices changes will make this approach more costly than a simple federated solution.

## Summary

---

There is no solution that fulfills all the requirements.

The centralized identity provider meets all the requirements except for the “institutional autonomy”. Every requirement is rated with green; but the drawback in this option is the migration costs of the existing institutions which have already implemented local LDAP solutions.

In a completely federated identity solution, the “institutional autonomy” is maintained, but falls short on the “one user name, one password” per user. In the federated solution, a user may have different user name and passwords at each institution. The user can synchronize their passwords manually; but this is time consuming for the end user.

In the centralized identity with institutional identity provider, the best of the first two options are merged. A user will receive a common user name and password at all institutions. Each institution maintains its own LDAP server. A central portal will alleviate the password synchronization issue for the user. By having a NSHE wide user name namespace; there is a higher probability of a name collision. As a result, users will need to change their user names in order to migrate to the new environment.

The name collision issue can be minimized by only using a centralized identity if the user requires access to multiple institutions. In this solution, the user name namespace remains at the institutional level. The probability of a name collision is reduced. This is the best option that meets the requirements.

The use of InCommon is the same as the federated identity solution. It has the same issues as the federated identity solution. In addition to those issues, the institutions must meet the security requirements of the InCommon federation and an initial fee and yearly recurring membership fees.

## Appendix A – Resources Consulted

Resource Consulted	Organization	Subject Matter or Title
<i>Ms. Robyn Render</i>	NSHE	Vice Chancellor of Information Technology
<i>Mr. Paul Mudgett</i>	NSHE	System Security Officer
<b>Mr. Chris Gaub</b>	NSHE	Director, System Support Services
<b>Mr. Mike Smith</b>	NSHE	Manager, System Support Services
<b>Mr. Steve Zideck</b>	TMCC	Director, Information Technology Services
<b>Mr. John Nicpon</b>	NSC	Computer Support Center Manager
<b>Mr. Ken Sullivan</b>	WNC	Director, Library and Instructional Technology
<b>Mr. Jim McKinney</b>	UNR	Director, Computing and Telecom
<b>Mr. Jeff Cox</b>	GBC	Director, Computer Services
<b>Mr. Don Diener</b>	UNLV	Associate Vice Provost for Information Technology
<b>Mr. Brian Chongtai</b>	NSC	Director of Information Technology
<b>Mr. Paul Pellegrino</b>	CSN	Security/Server Administrator, Technology Services
<b>Mr. Jeff Springer</b>	UNR	Active Directory
<b>Mr. Chris Mercer</b>	CIBER	Project Director
<b>Ms. Carol A. Dahlin</b>	CIBER	Senior Practice Manager
<b>Ms. Tasleema Lallmamode</b>	Arizona State University	Technical Analyst
<b>Mr. Tim Larson</b>	University of Central Florida	UCF Computer Services & Telecommunications

## Appendix B - Oracle PeopleSoft Solutions

---

Oracle PeopleSoft has three options to enable a single sign on (SSO).

- PeopleSoft only

This option enables single sign on only between multiple PeopleSoft applications. After a user is authenticated by one PeopleSoft application, an in-memory value gets set in the browser that the next PeopleSoft application uses as a user credential.

This option will work for sign on to multiple PeopleSoft instances and applications.
- Oracle as a Trusted Node

Use this option if both Oracle and PeopleSoft applications are being used. Once a user has been authenticated by the Oracle system, they can freely access PeopleSoft applications without having to re-authenticate.

This option is tailored for sites running PeopleSoft application on BEA WebLogic or IBM WebSphere servers.
- Oracle as a Partner Application

This is the recommended option if the PeopleSoft applications are installed on Oracle Application Server 10g.

This option is **not** available on BEA WebLogic or IBM WebSphere.

This option has the end user signing in through the Oracle Single Sign on server.

This option will enable other applications to re-use the SSO server infrastructure and thus be SSO enabled.



## **Appendix C - Arizona State University**

---

Arizona State University (ASU) has a single user id for all their systems; it is based on the EMPL\_ID from PeopleSoft.

Currently there is a batch process that extracts the EMPL\_ID from PeopleSoft and feeds an internal system to provision the ids in LDAP and Active Directory.

ASU is using a home grown SSO system called WebAuth. The authentication is based on Kerberos backed by Active Directory. ASU is currently implementing Central Authentication Service (CAS), but are not sure how to size the CAS server to support all their students and systems.

SSO for PeopleSoft was implemented using the capabilities of PeopleSoft systems within the portal.

The provisioned id remains with the student for "life"; when the student graduates and becomes an alumnus, the id is used to access alumni resources.



## **Appendix D - California State University**

---

California State University (CSU) campuses all joined the InCommon federation. At CSU, the problem statement is similar to the issues at Nevada System of Higher Education except for the single user name and password. See the white paper from InCommon at [http://www.incommonfederation.org/docs/eg/InC\\_CaseStudy\\_Cal\\_State\\_2010.pdf](http://www.incommonfederation.org/docs/eg/InC_CaseStudy_Cal_State_2010.pdf).

CSU had heterogeneous technologies across all their campuses. Each campus managed their technology independently with a few centrally administered systems.

With InCommon, CSU was able to implement a “private” federation of its own campuses.

CSU initially piloted access to shared library resources for faculty and graduate researchers. As of the writing of the white paper, CSU federate its financial systems, data warehouses and Microsoft SharePoint.

## Appendix E - University of Central Florida

---

The University of Central Florida (UCF) uses a single institution approach.

UCF has:

- Single instance of PeopleSoft
  - The PeopleSoft authenticates against a Sun LDAP server
- PeopleSoft extract changes and loads the new records into the LDAP server. The load has a Network ID (NID) and a Person ID (PID). Both are loaded into the LDAP server
- UCF is using the PeopleSoft supported SSO between PeopleSoft systems on the portal
- Have custom java code for Blackboard to integrate with LDAP server
- Considering using Sun SSO to integrate more applications at the web level

For federated services, they are looking at:

- Microsoft FIM
- Shibboleth
- InCommon

UCF plans to have an implementation by Jan 2011

Their campuses all authenticate against a common LDAP server.