Identity and Access Management – Current State and Considerations for Prospective Students

Version 1.0 - August 2015
Table of Contents

Purpose of this Document ........................................................................................................... 3
Executive Summary ......................................................................................................................... 3
Current Situation ............................................................................................................................... 4
Identity Data Collection and Processing ......................................................................................... 4
  Identity Verification ......................................................................................................................... 5
  Identity Reconciliation ..................................................................................................................... 5
  Identity Linking ............................................................................................................................... 5
  UAI Allocation ............................................................................................................................... 5
  Credential Generation ..................................................................................................................... 6
Group Allocation and Ongoing Membership Assessment ................................................................. 6
Identity Data Usage .......................................................................................................................... 7
  Active versus Terminated Accounts .............................................................................................. 7
  Authentication ............................................................................................................................... 7
  Affiliation Types ............................................................................................................................ 8
  Same & Single Sign-On .................................................................................................................... 8
  Authorisation ............................................................................................................................... 8
  Personalisation ............................................................................................................................. 8
CSU Identity Management Architecture Concepts ............................................................................ 9
  Community Boundaries ............................................................................................................... 9
  Affiliation Lifecycles ..................................................................................................................... 9
  Identity Data Retention and Transience of affiliation .................................................................... 9
The CSU Identity Management Roadmap ....................................................................................... 10
Issues and Challenges of including prospects in the CSU IAM Process ........................................ 10

Table of Figures

Figure 1 Distributed IAM Architecture ......................................................................................... 4
Figure 2 Web-Methods middleware - Automated Groups ............................................................... 6
Figure 3 Group to Service relationship .......................................................................................... 7
Figure 4 Identity collection and processing flow .......................................................................... 7
Figure 5 CSU IAM High-Level Architecture ................................................................................. 9
Figure 6 Identity affiliations and lifecycles .................................................................................... 9
Figure 7 Identity application boundaries ..................................................................................... 11
Purpose of this Document

The purpose of this document is to describe the current Identity Management landscape at CSU and to discuss the potential impacts relating to the inclusion of prospective students into the Identity Management Processes of the University.

Executive Summary

Identity and Access Management (IAM) or sometimes referred to as Identity Management (IDM) is the process of capturing and storing data relating to people that have an affiliation with an organisation and using information relating to the nature of that affiliation to control access to services and provide a personalised experience for the duration of the affiliation.

IAM is an extremely complex process that draws data from many contributing systems and has to cater to the intricacies of the systems dependent on it. At CSU this is further complicated by being in the throes of progressing through a major roadmap of activities to move from a legacy system to a much more advantageous future state.

To date prospective students (Prospects) have not been included in the scope of Identity Management at CSU. While identity data is collected and managed in CSU systems such as the Customer Relationship Management (CRM) system and the Student application process, prospects have not been granted access to other CSU systems and therefore have not required the creation of a User Account\(^1\) that can be used to log in to those services.

Current strategies aimed at improving the conversion rate of Prospects to Enrolled Students are providing impetus to enhance the management capability of these identities, to improve the user experience and to provide analytical data that can help improve conversion rates.

The introduction of Prospects will introduce significant challenges that will require changes to both business and technology processes. This discussion paper does not attempt to identify solutions but provides a view of the current IAM environment at CSU and tries to articulate some of the challenges that will need to be resolved.

---

\(^1\) A user Account is a term that refers to an Identity that has access to a service. It consists of a user profile (attributes of the person) and a set of credentials (usually a Username and Password).
Current Situation

Identity Data Collection and Processing

The CSU IAM process including supporting applications and services is complex and continually changing to meet the needs of the business. Recent investment has seen substantial progress, moving away from a legacy system developed in the late 1990’s toward a much improved Identity and Group Management System (IGMS) that offers greatly enhanced management features and the ability to dynamically group people based on business rules. While this is a significant step, IAM at CSU has much further to progress to meet the challenges that have risen over the past few years.

The IAM architecture adopted at CSU is a distributed rather than centralised model. In a centralised model identity data is captured in a central IAM application that reconciles the identity against all existing identity records, establishes an identity record and then distributes the details to the appropriate dependant Information Systems.

In the distributed approach taken at CSU the identity data is collected in contributing applications (Identity Gateways) relevant to the person’s affiliation with the university and is then transferred in real-time, using the Universities middleware Web-Methods, to a central identity repository where:

- It is reconciled against existing identities
- The identity is linked to Identity records in Identity Gateways
- Allocated a Unique Arbitrary Identifier (UAI)
- Credentials (Username & Password) are generated
- Automatically allocated to appropriate groups

![Distributed IAM Architecture](image)

The three current Identity Gateways at CSU are:
- Banner Student/Finance – Students and other people that are invoiced etc.
- Alesco HR – Staff of the university and others that are paid stipends etc.
- Temporary Access System - Additional users that are not managed in the other gateways. E.g. CSU-Advance Students and Third Parties that access CSU services.

*Note: These can be added by any Staff Member.*
Identity Verification
Identity verification is the process of confirming an identity is who they claim to be. At CSU this is generally done at the point of data collection in the Identity Gateway system by administrative staff in either HR, Student Administration or Finance. Verification processes range from sighting photographic identification through to the collection of documentary evidence such as birth and marriage certificates or evidence of previous study or qualifications. Even with the Temporary Access System the identity has a relationship with the staff member creating the identity record and is linked to that new identity in a supervisory role. There is increasing emphasis being placed on rigorous identity verification processes by groups such as the Australian Access Federation (AAF) who facilitate access to services hosted by other organisations particularly in the field of research.

Identity Reconciliation
When the identity data is copied to the IGMS an Identity Matching process is executed that matches key identity attributes such as Names, Gender, Date of Birth, and Gateway Identifiers against all identities stored in the repository. The matching process uses rules stored in database tables that can be enhanced and modified over time to improve the reconciliation process. Potential matches are flagged for manual resolution through the IGMS user interface.

Identity Linking
There are three main scenarios for identities coming from Identity Gateways.

1. There is no potential match with an existing identity record so a new IGMS record is created and linked to the gateway identity.
2. There is an exact match with an existing IGMS identity record so no new identity record is created but the existing IGMS record is linked to the gateway identity.
3. There is a potential match (based on the reconciliation rules) which is flagged for manual intervention by administrative staff prior to continuing. There are 3 resolution options:
   a. Determine the identity already exists and link it to the gateway identity
   b. Determine it is not a match and create a new IGMS Identity
   c. Resolve the issue by fixing the data in the gateway system.

UAI Allocation
For all new identity records created a Unique Arbitrary Identifier is created. This is referred to as the CSU_ID. It is a sequentially allocated number that is application agnostic and acts to link together the Identity data attributes in the IGMS as well as linking them to the identifiers of the gateways. The UAI is unique to each identity and remains unchanged for that identity for the duration of their association with CSU.
Credential Generation
For each new IGMS identity record a set of credentials are generated and consist of:

Username:
- A unique string of characters used as the known value in a value-pair used to prove a person’s identity.
- Is currently based on name and uses a one pattern for Students and another pattern for Staff and other identities
- Can currently change over time under some circumstances.

Note: ii & iii will no longer be true with the introduction of Numberplate Usernames.

Password:
- Initially generated as a random string of characters used as the secret value in a value-pair used to prove a person’s identity.
- Students are not required to change their password after they have activated their account and set their password for the first time, although they can if they wish. Staff and others are required to change their password every 60 days.

Group Allocation and Ongoing Membership Assessment
All identities in the IGMS are assessed for membership of Automated Groups. Group membership is determined by rules that have clauses based on attributes from gateway systems using the Dynamic Rules Management System (DRMS). The Rule Management interface is integrated into the IGMS user interface. Web-Methods monitors the gateways for changes in data relating to the identity e.g. position changes for staff or enrolment changes for students. When data changes messages are sent to the IGMS, group membership is re-evaluated and modified based on the rules.

Some simple example in IGMS include:
- Postgraduate Student
  - Enrolment Status = “AS” (Active Student)
  - Course Level = “PG” (Postgraduate)
- Academic Staff
  - Position Category = “ACAD” (Academic Staff)
  - Termination Date > “Today” (Current Employed)

For example if a staff members Position Category changed in Alesco from “ACAD” to “CASG” (Casual General) they would be removed from the “Academic Staff” group and would become a member of the “Casual Staff” group.

Group Membership is controlled by using dates. Each membership has an “Effective From” date and an “Effective To” date (this can be pre-populated or left empty until a change happens to terminate the membership. Identities can be in none or many groups concurrently e.g. an identity could be in the “Staff”, “Academic Staff”, “Student” and “Undergraduate Student” groups at the same time.
Special Groups referred to as “Services” can be linked/mapped to one or more groups. Service membership is the superset of the members of the groups to which it is linked. Services can be used to control access to Applications or Services. For example to control access to the EZProxy system for Library resources a Service called “EZProxy Access” can be linked to the “Staff” and “Student” groups resulting in the combined members of the two groups in the membership of the service. Services are designed to provide a mechanism to link multiple groups together when the membership of any of the groups change this is reflected in the Service membership.

Figure 3 Group to Service relationship

Identity data collection and processing involves the following process steps. These do not necessarily happen sequentially in the order shown. Some steps are automated and others require manual intervention.

Figure 4 Identity collection and processing flow

Identity Data Usage

Identity data collected in the Identity Repository (IGMS) is used for several purposes including controlling access to applications and services, automated roles to control application functionality based on automated group memberships, personalisation of user experience and targeted content delivery.

Active versus Terminated Accounts

CSU User Accounts in the CSU IAM architecture are considered “Active” when it belongs to groups that provide access to Services. When an identity is no longer a member of any of these groups they are no longer considered “Active” and therefore are considered “Terminated”. Being terminated has the effect of removing access to the majority of applications and services.

Authentication

Authentication is the process of ensuring a person is in fact who they claim to be by checking their entered credentials against those on record. An identity must authenticate before gaining access to a restricted application’s user interface by entering their username and password. CSU currently employs a wide range authentication methods but in general the credentials are used to connect to a Directory Service\(^2\) such as OpenLDAP or “Active Directory” for comparison.

\(^2\) A Directory Service is a specialised hierarchical data repository that is optimised for reading. It contains identity profiles and access privileges. It is usually implemented in a highly available architecture.
Affiliation Types.
While the IGMS system allows for more granular definition of Affiliation types the legacy system only allows two types; “Staff” and “Student”. This is implemented as a simple flag that has only two values. In addition to this restriction you can only be one or the other at any given point in time. This means generally for those that are both staff and student, the Staff affiliation takes precedence. Currently anyone that does not fit either of the two options is flagged as Staff. Prospects could not be considered as either and a solution would need to be found to address this limitation.

Same & Single Sign-On
CSU generally uses the same set of credentials across applications and services although there are some exceptions that stand apart from the Identity Management process using locally managed accounts.
Using common credentials when authenticating to applications is referred to as “Same Sign-On” the user still logs on to each application every time but uses just one set of common credentials. With “Single Sign-On” a token system is used. The user authenticates once and is granted a token that lasts for several hours. The token can be used to gain access to multiple systems without re-authenticating for the life of the token. Most Student-Facing applications at CSU use Single Sign-On via software called Shibboleth. This is also used for Federated authentication with the AAF so once authenticated a CSU user can avail themselves of any service offered through the federation.

Authorisation
Once an identity is authenticated they can start using the Applications functionality. An individual’s rights and permissions within an application or service are often controlled by groups and system roles. For example Interact2 is segregated into many sites which have an Instructor role, a Learner role and a Site Administrator role. Each of these roles have different permissions. IGMS automated groups are used to populate Interact2 site roles. Web-Methods is used to provision the Interact2 using the Master Data definitions for Enterprise Groups and Services in real-time.

Personalisation
IGMS groups can be used for personalisation of the User Experience in applications as well. Groups based on Campus, Course Level, Study Mode etc. have been established that are used to provide different content in the Student Portal based on group membership. Like all automated (Dynamic) groups the membership is based on rules and is re-evaluated when an identity’s attributes change.
CSU Identity Management Architecture Concepts.

Community Boundaries.
Identities currently considered part of the CSU Community consist of Staff, Students and a limited number of people with non-traditional affiliations to the University. Each of these groups has a different lifecycle of association which aligns with their need to use CSU Applications and Services. Identity types that fall outside these traditional boundaries and lifecycles, currently need to be managed differently to ensure they do not get services they would normally receive by virtue of being part of the CSU Community.

For example AAF services that are provided to all CSU community members based on the premise they are Staff, Students or some other close relationship with the university and this happens to correspond with the identity types we manage in our IAM solution. The authentication of users has not been built to discriminate between different identity types because they are all currently eligible. If other identity types are introduced into our IAM process and systems, the authentication and authorisation to the AAF service will need to be modified to be more selective.

Affiliation Lifecycles.
Identities have a defined lifecycle in line with their affiliation. Staff are employed then resign or retire, students are admitted and then graduate or withdraw, and others have a manually set period of affiliation. The timeframes of the lifecycles vary i.e. a staff member could be employed for 2 weeks or 40 years but they have a clear start and end point to their association and correspondingly when they require access to services, and when they should no longer retain that access. This is achieved via the concept of the “Active” and “Terminated” Accounts. Once terminated an identity cannot use our existing authentication methods to gain access to services.

Identity Data Retention and Transience of affiliation
Privacy legislation states:
“Entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed”
Identity data is currently retained at CSU indefinitely based on the premise that having been a member of the CSU community there is a lifetime engagement through alumni or through lifetime learning for students. Data relating to Identities that only have a cursory relationship with CSU and may not ever progress to a traditional affiliation may not fit this criteria.

3 Students are granted an additional 18 months of access through membership of the “Past Student” group after termination of their study.
The CSU Identity Management Roadmap

While significant progress has been made on enhancing the Identity Management Process at CSU there is much that remains to be done to match the level of process maturity and capability to the university’s strategic outcomes. The original CSU IAM software tools were developed in the late Nineties and have evolved organically over the years as new circumstances have arisen. While new tools such as the DRMS and the IGMS have been developed and identity data movement has been made real-time by using the Web-Methods middleware, much of the process is still rooted in the legacy IAM system. This complex mixture of the new and legacy system make dealing with non-traditional affiliations difficult.

Relevant issues identified in IAM Roadmap

| Group Functionality in OpenLDAP Directory Service | While new LDAP infrastructure that provides group functionality is now in place no applications have been migrated to the new version. Authentication is still pointing to the old LDAP version that does not allow access control based on groups. |
| Username are still being created in Legacy formats. | Current username formats have issues that would be further exacerbated by a significant rise in identity numbers. |
| Password Management | Password management at CSU is not best practice and is currently provided from the Legacy System. This makes self-service activation and password resets etc. less than ideal and which results in additional workload on support staff to deal with password issues. |
| Assurance Levels. | Federation Service providers are increasingly demanding better levels of identity verification before providing access to their services. The AAF has indicated that some Research Service providers will soon insist on physically sighted photographic identification to reach the appropriate Level of Assurance. There is currently no method to distinguish different levels of Identity Verification in the System. |
| Directory Service provisioning. | While OpenLDAP is currently provisioned directly from the IGMS system, Microsoft Active Directory (AD) is currently provisioned from the legacy system. No IGMS groups are populated into AD although course grained groups are derived from legacy system data. |
| Non-Current Identities | Identities that fall outside the Affiliation and Lifecycle boundaries are currently excluded from the authentication process. So people having a prior association with CSU are explicitly from all services. Roadmap items that move away from the legacy system will improve the ability to manage these issues. |

Issues and Challenges of including prospects in the CSU IAM Process

In order to introduce Prospect identities into the IAM process there are some fundamental issues that need to be resolved. While not attempting to identify solutions the following is a discussion of those issues. Identity capture in pre-admission systems is primarily done via self-service registration with little or no reconciliation and no identity verification. Because prospects may never further engage with CSU we need to exclude them from CSU applications and services beyond the Pre-Admission systems, while implementing a common identifier layer across all levels of engagement to facilitate ‘Prospect to Enrolment’ tracking for Analytics and allow data movement between systems. We also need to provide a common Authentication method and credential set to allow a better student experience by allowing existing students the ability to use their CSU credentials and identifiers to access the Application or Credit Precedence applications as well as preventing the need to switch them when transitioning from Prospect to CSU identity.
**Figure 7 Identity application boundaries**

**Pre-Admission**

Applications used to discover, recruit and manage prospects as well as allowing the prospect to interactively make course and study enquiries can be classed as pre-admission systems. Engagement with these systems is for a new identity that is typically a precursor to the admissions process where the traditional student identity lifecycle begins. Identity records are generally created through a self-registration process with little or no Identity verification or reconciliation.

**Protected Services**

Prospects are likely to be unverified, and unreconciled and need to be excluded from accessing both CSU and other Federated Services until their engagement with CSU progresses to a more trusted affiliation. This will mean that all protected services will need to determine appropriate access approval over and above simple authentication.

**Multiple entry points for Prospects**

Prospects may initiate engagement with the pre-admission process through multiple paths. Either through the CRM (Web Form or Phone), the Credent Precedence application or through the Application process in Banner Self-Service or via a UAC/VTAC process. This may happen over a short time frame or be over a much longer period with multiple disparate occurrences.

**Identity Stages**

Prospects can be in three stages of their affiliation with CSU. Past – Have had a prior Identity Account but are not currently active. Existing – Have a current Active Account. New – Have no prior Account with CSU. Each of these scenarios present individual challenges in Account (re-)activation and management.

**Common Identifiers**

In order to achieve the objectives of maintaining prospect to enrolment analytical data as well as allowing meaningful data exchange between pre-admission and post-admission systems there needs to be either a common unique identifier used across all systems or a way to link disparate identifiers between the systems.

**Common Authentication**

In addition to a common identifier layer a common authentication layer is required for a seamless user experience. Past, Existing or New identities need a common and consistent set of credentials regardless of their current level of engagement. This needs to be supported by common IAM processes such as Account Activation and Forgotten Password reset processes etc.

**Lifecycle of engagement**

Prospects that have had no prior affiliation with CSU have no defined lifecycle. A balance must be struck between privacy legislation and the need to retain data long enough for a prospect to re-engage without having to resubmit previously provided data.

**Identity Verification**

Un-vetted Self-Registration processes are open to abuse from manual and automated malicious intent. Creating of bogus accounts can be mitigated by a process of sending an
email to a nominated email address prior to continuing the registration process. Of course there is no verification process for the creation of free email accounts. This emphasises the need to exclude prospects from other CSU services.

Identity Reconciliation

The introduction of prospects to the identity management process adds significant Data Quality challenges. The number of potential matches with existing identities is likely to rise substantially. A decision needs to be made on the point of reconciliation i.e. is reconciliation deferred until admission phase is reached or try and reconcile at registration to ensure data quality throughout the progression of a prospect. The later would be difficult without direct contact with the prospect.