Colorado School of Mines Project Plan

Executive Summary

Colorado School of Mines (“Mines”) deployed a commercial Identity and Access Management (IAM) solution in 2015, replacing an aging, internally-developed system. As a result, Mines is able to automatically provision role-based access across the majority of internal systems for accepted student applicants, new students, and employees. The same solution provides a user portal for self-service password management. Mines is a member of InCommon and has relied on Shibboleth since 2013 for providing federated IDP and SP services. Mines already has an active IAM project plan that calls for deployment of greater functionality in this area – including the implementation of Grouper for automating and delegating group-based access and the migration of its existing person repository to a more robust entity repository such as midPoint.

Recent concerns around the viability of the commercial solution demand that Mines re-examine its direction with respect to an internal IAM solution. As the vision and direction of TIER has matured, it has become clear that Mines would benefit from implementing TIER and becoming an active participant in the TIER community. The TIER architecture and integrated components would allow Mines to provide a greater level of identity and access services to its students, researchers, faculty, and staff that interoperate with the research and education community. The TIER Campus Success Program will provide a collaborative environment with technical resources, knowledge transfer, and training that will enable Mines to alter its course around identify initiatives towards the TIER ecosystem. It would also allow Mines to simultaneously contribute to this community driven initiative in a manner that would benefit future institutions.

Organization Description

Colorado School of Mines is a public research university in Golden, CO, with academic programs and research portfolio devoted to engineering and applied science. It has the highest admissions standards of any public university in Colorado and among the highest of any public university in the U.S. Mines has distinguished itself by developing a curriculum and research program geared towards responsible stewardship of the earth and its resources.

In addition to strong education and research programs in traditional fields of science and engineering, Mines is one of a very few institutions in the world having broad expertise in resource exploration, extraction, production and utilization. As such, Mines occupies a unique position among the world's institutions of higher education. The world faces a crisis in balancing resource availability with environmental protection and Mines and its programs are central to the solution.

Mines offers all the advantages of a world-class research institution with a size that allows for personal attention. Current enrollment in Fall of 2017 is 6,043 which is comprised of 79% undergraduate and 21% graduate students. Computing, Communications, and Information Technologies (CCIT) offers centralized support for technology strategy and all institution-wide technology initiatives, projects, and services at Mines. This centralized approach works extremely well, particularly given Mines size (student, faculty, and staff population). Among other benefits, it affords an opportunity for standardization around approaches to technology and technology platforms - including identity management, access management, and the integration of disparate systems.

Containerized TIER Component(s) to be implemented

- Grouper Access Management Software
- Entity Registry, such as midPoint

Short Management-Level Use Case Description of Your Project

Mines currently has a functioning vendor-based solution for identity management, including a person registry, provisioning of accounts across multiple service platforms, fundamental role-based access control, and password management. The solution successfully manages 90% of all automated provisioning across a variety of disparate systems. Users are able to utilize a self-service portal to claim an account as well manage password changes.

There are, however, several functional shortcomings in the existing solution. First, all de-provisioning of accounts is done manually. Additionally, Account provisioning is based on high-level Banner institutional roles and does not have the granularity required to manage access to resources at the level required. Such requirements include lab and classroom access for students based on major and/or course enrollment, access to software and services based on affiliation, membership in various groups

and mail lists based on job title, job function, major or department, and various levels of access to Banner and associated applications based on job title and function. Specifically, Mines would like to move from a role based access control model to attribute based access control. Lastly, all sponsored user accounts such as those for visiting faculty, visiting students, vendors and contract employees are manually processed.

The currently active IAM project roadmap includes initiatives to address these identified shortcomings, including automated de-provisioning within the system and subsequent implementation of Grouper to address institutional requirements surrounding access management. However – and perhaps most critical - there is a great deal of concern around the current vendor and the future viability of their solution. As a result, Mines has been exploring options for a replacement IAM solution.

Scope

Inclusions:

- Installation and configuration of midPoint as an entity registry
- Development of midPoint as self-service portal for password management
- Integration of the existing source of authority (Banner) for person records with midPoint
- Integration of end-point services with midPoint for provisioning / de-provisioning of accounts
- Migration of current functionality within existing IAM solution (including provisioning, de-provisioning, and password self-service) from existing IAM to TIER components
- Training of all stake-holders on new platform, from technical support to functional use

- Installation and configuration of Grouper
- Pilot use of Grouper for finer-grained role-based access
- Migration of Grouper to production environment for pre-selected systems/resources

Exclusions:

No other work will be done that is not expressly described in the inclusions.

Key Stakeholders

Sponsor:	Mike Erickson, CIO
Campus Success Program Contact(s):	Mike Erickson, CIO
Communications contact:	Matt Brookover, IAM Architect
Project Manager	Clayton Durkee, Project Portfolio Manager
Project team members:	Matt Brookover, IAM Architect Ginny Lee, IAM Support Yuri Csapo, Server / Operations Admin, (tbd), Banner Integration Specialist
Deployment Partners/Contractors	[name]

Project Milestones:

Key Milestones	Assigned Resources	Start Date	End Date
Project Charter Complete	Clayton Durkee	Present	Mid Oct
Project Plan Complete	Clayton Durkee	Mid Oct	End of Oct
Technical Training Complete	Identified Team members	*	*
midPoint installed/ configured/tested	Matt Brookover	*	*
midPoint migrated to production	Matt Brookover	*	*
Grouper installed/ configured/tested	Matt Brookover	*	*
Grouper migrated to production	Matt Brookover	*	*

* - to be determined as planning is completed

Synergistic Projects

N/A

Constraints, Assumptions, Risks and Dependencies:

Constraints	Resources are constrained by other work
Assumptions	Support from the Campus Success program will provide technical resources and collaborative environment to assist in the installation, configuration, and adoption of the identified technologies.

Risks	1. Personnel / SME resources may not be available for project because of other demands 2. Personnel resources may not have the needed expertise 3. Support (information) from program may not be as expected 4. The software is harder than expected to learn and may delay development and adoption 5. The integration to Banner or other software and services takes longer than expected, delaying development and adoption 6. The system does not operate as expected, leading to additional effort
Dependencies	Project is appropriately prioritized