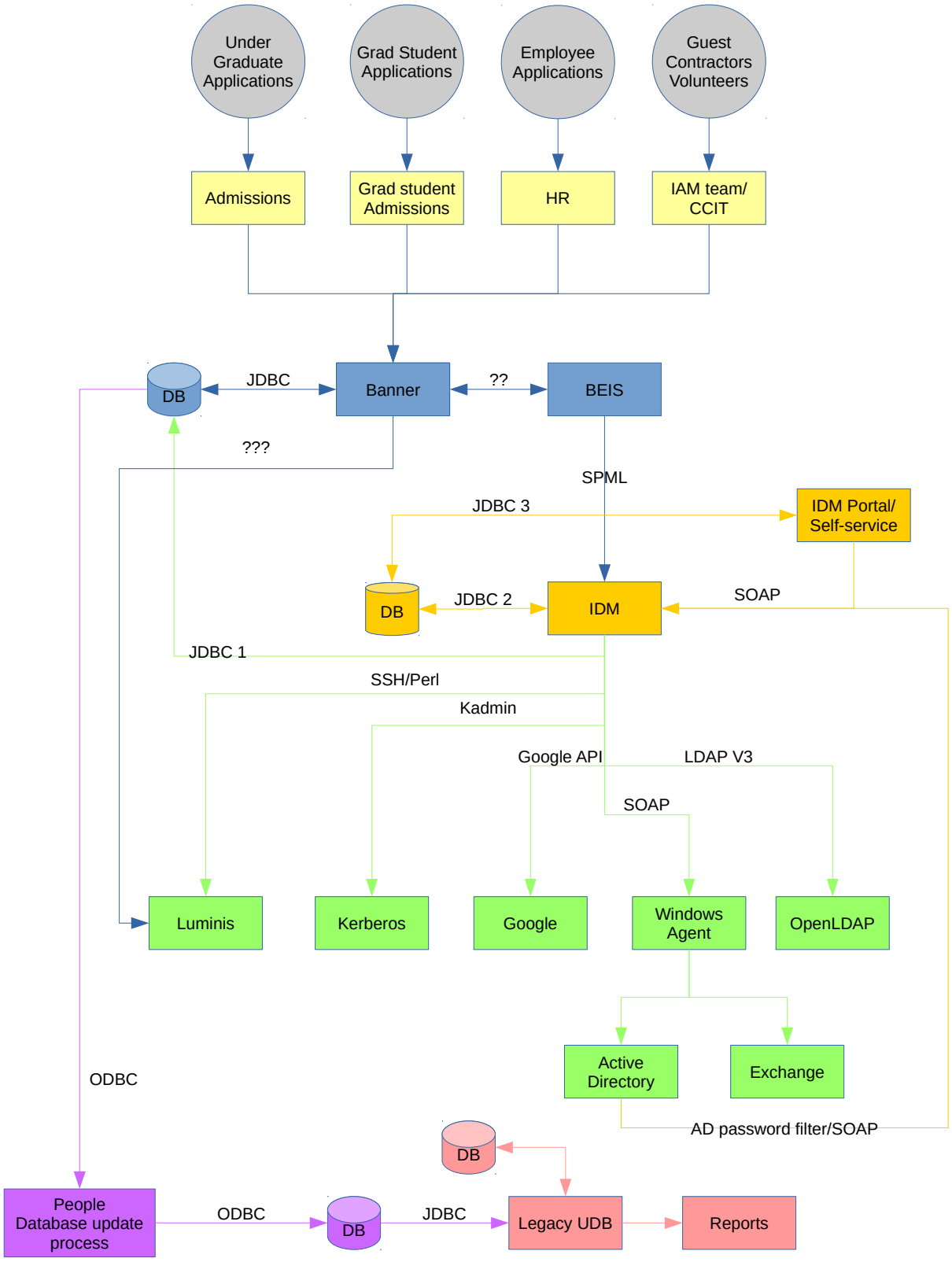
IAM Functional Model



Applications

Potential members of the Mines community can apply to be a student, faculty, staff, grad student, guest, contractor or a volunteer. These applications are processed by the admissions departments, Human Resources, or the IAM team in the IT department. At some point, a record will be entered into Banner. If there is an existing record for that person, the existing record will be used. If this is a new user, a CWID (Campus Wide ID Number) is assigned. So, if you were a student, graduated, left the school and then apply for a job as a researcher, you will have the same CWID that you were assigned as a student.

Banner

Mines uses Ellucian's Banner ERP to manage information on students, employees, guests, process applications, etc. Banner serves as Mines primary system of record (SOR).

Banner has a module called Banner Enterprise Identity Service or BEIS. BEIS implements the Service Provisioning Markup Language or SPML. SPML is also supported by the Identity and Access Management System, IDM. Every time an identity record is updated in Banner, an SPML message is sent to the IDM. This event driven model has worked well to keep the IDM in synch with Banner.

SPML

The SPML message includes the persons name, the university email address used for official communications, application decision codes, user name (aka EXT_ID, Banner third party ID, or NetID), employee classification, employee department code, employee start date, employee last date worked, employee termination date, graduation date, institutional role, and the Banner UDCIdentifier.

There is enough data to determine if the user is allowed to claim an account, but not quite enough to de-provision accounts or re-provision the account for a returning user.

The IDM will decode the message from Banner and then kick off a number of operations. First, update its own copy of the record and then push updates to Active Directory, OpenLDAP, Google, etc. The updates can be something simple like changing the user's last name, or more complex like setting roles and granting access to more systems.

IDM

Mines current IDM was purchased from a vendor that has gone out of business. The IDM implements role based access control (RBAC) system. Features include:

- role based and rule based access controls, rules are implemented in Groovy
- automated workflow

- password management
- useful mix of connectors to LDAP, Google, Active Directory and the ability to use Groovy to add others, such as Luminis.
- workflow that implements self-service features:
  - account claim
  - password change
  - recovery of forgotten passwords
  - ability to set or change answers to password recovery questions and an email address or SMS phone number for password recovery.
  - ability to set a password for Google's IMAP or POP service

The account claim workflow is also a system of record. The account claim workflow is used to generate user names, email addresses and gather answers to password recovery questions, only the user name and email address is sent back to Banner when the user claims the account.

Self-Service Account Claim Workflow

New Mines users are sent to the self-service account claim web site. This web site implements a workflow that will set up the users account on various Mines systems. During the on boarding process, the user will receive their Campus Wide ID (CWID) number, and will need it for the account claim.

For students, faculty, staff and various guest roles, the claim process will walk the user through a set of forms:

1. The first form will ask the user if they agree to Mine's acceptable user policy, if they agree, they move on, if not, the process exits.
2. The second form will collect name, CWID and birth-date.
3. The workflow will use the CWID to look the user up in the IDM using a SOAP based API. The workflow will then compare the name and birth-date to the record returned by the IDM. If the name and birth-date match what was provided by the user and if the user is eligible to claim an account then the user will go on to the next form, or they will get an error with a suggestion to open a help desk ticket – see below for a details on some of the eligibility checks.
4. The next form will let the user choose a user name. The form presents 5 available user names based on various permutations of the users full name, allows the user to pick one and then click next.
5. If the user chooses to provide account recovery information, a form is displayed that requests a cell phone number, phone company (AT&T, Verison, T-Mobile, etc), an email address, and the answers to 5 questions.
6. After collecting the recovery information, the next form will request the users password.

7. The last step, the workflow will send this information back to the IDM using the web service API.
8. At this point, a final screen is displayed to the user with the user name and the IDM starts setting up the accounts.

To trigger the account setup process, the self-service account claim workflow will use the IDM web service API to set provisioning roles in the IDM that are based on Banner institutional roles. The Student and Employee IDM roles will add entries to OpenLDAP, Kerberos, trigger Banner to create the Luminis account, and add a user in Active Directory. The gmail role is used primarily for students, and will set up the Google G Suite account.

Student Application and On-boarding

When a person applies to be a student, their application is processed by either the undergraduate or graduate student admissions office, and after various steps are admitted. Some one in that office will add the admitted flag to that students application decision code in Banner. Banner sends an SPML message to the IDM with that change. Also, a letter is sent to the student to let them know they have been admitted and outlines several steps. One step is to reply to the admissions office to signal their intent to enroll. Another step is to claim the account, log into Luminis and look at the financial aid shopping sheet which outlines the cost of attending the school.

To log into Luminis you must have a user name and password. Only Banner can provision a user in Luminis. When the Banner third party ID (aka user name) is set, Banner will send a message to Luminis to create the user. The new Luminis user does not have a password so the user will not be able to log in. When the user claims the account in self-service, they choose a user name and password. The account claim workflow sends that information to the IDM along with the users new role. When the Student or Employee role is assigned, the IDM uses the JDBC 1 connector to add the user name in that users third party ID in Banner. This triggers Banner to provision the user in Luminis. At the same time, the IDM also sets a flag that will allow the password to be sent from the IDM to Luminis. The password must be sent after the account is created by Banner, so there is a delay that can be as long as 5 minutes before the password is released to Luminis. It is also possible that there could be other updates in queue ahead of the message that causes Luminis to provision the user. The IDM only sends passwords to Luminis users every 5 minutes, but, if there is long message queue, it could be more than 5 minutes before the new Luminis account and password are provisioned.

If the user claims the account when they have the admit application decision codes only Luminis is provisioned. At some point, they will either drop out of the process or signal their intent to enroll. When the admissions offices receives a message from the student that indicates they intend to enroll, and when the check or credit card charge clears, someone in the admissions office will add the APDC (Application Decision Codes) code to the users record in Banner. Banner will send a new SPML message to the IDM. If the user has claimed the account, the IDM will add a mail box in Google,

entries in Active Directory, LDAP, and Kerberos. At this point, the new student can show up to the first day of class, log into lab workstations, etc.

Some students will run the account claim after they have signaled their intent to enroll. In this case, the Luminis account, Google mail box, Active Directory, LDAP and Kerberos entries will be created when the account is claimed.

Student Account Claim Eligibility

The Banner APDC contain many useful details that include the term the student expects to start classes, a code that indicates if they are an applicant, were admitted, signaled their intent to enroll, deferred to a later semester, or withdrew from the process.

The claim process will allow a student to claim if they have an APDC code of admit or intend to enroll and the date that the user ran the claim process is before the last day of the first month of the term that they applied to. If that criteria is not met, or if there is a deferral or withdrawal code, the account claim workflow will stop and let the user know they cannot claim and suggest they open a help desk ticket. If the user meets the criteria, then they will go on to the next step which is to pick a user name.

Employee Account Claim Processing

Employees are much simpler then students. If you are an employee and the date that you run the account claim is less then 60 days after your start date, you can claim the account. The account claim workflow will run the same set of forms for employees that it does for students, and then set the employee role in the IDM. When the account claim workflow sets the employee role in the IDM, the IDM will send the user name and email address to Banner via the JDBC 1 connector, Banner will provision a Luminis account, the IDM will provision LDAP, Kerberos, Active Directory and an Exchange mail box.

Guests, Contractors, Volunteers, etc

There are many variations for these users. They start with a help desk ticket and end up with forms being processed and accounts provisioned. Most of these accounts are provisioned manually, forms are keyed into Banner, banner sends the records to the IDM. After the records are sent from Banner, an IAM admin will use the IDM admin interface to set the necessary the IDM roles. The CWID will be sent to the user and the user will be able to run the account claim.

Password Changes

There are several ways a user can change the password:

1. If the user has provided password recovery information in the self-service system, they can use the forgot my password service and change the password.

2. The user can go to self-service and enter the old password and a new password and the password will be changed.
3. The user can go to the TSC (Technology Support Center) present an ID and have a consultant change the password in the IDM admin interface.
4. The password can be changed on a windows workstation. The active directory password filter will capture the password and route it to the IDM.

No matter how the password is collected, the new password will be distributed to Luminis, Kerberos, and Active Directory.

We do not send passwords to Google or OpenLDAP. Google is configured to use Shibboleth, and Shibboleth uses Kerberos to authenticate the user. OpenLDAP also uses Kerberos to validate passwords or OpenLDAP will take a Kerberos ticket granting ticket to authenticate a user.

LDAP, Kerberos, Active Directory, Google, Banner

The IDM uses a number of different protocols to provision users into these systems. Technically, Banner has two connections to the IDM, one is the SPML feed to load new identity records into the IDM, the other is the JDBC connector that is used to send the user name and email address back to Banner.

The IDM uses various protocols to provision identity records in LDAP, Kerberos, Google, and Active Directory.

Windows Agent

The IDM technically does not talk to Active Directory or Exchange. The IDM sends various SOAP requests to an agent. The agent will process the request, figure out if it needs to change a password, add an account, etc. Appropriate power shell scripts are called to perform the actual changes to Active Directory.

When creating an account, if the email address is set to user@mines.edu the agent will also create an exchange mail box. For students, the email address is set to user@mymail.mines.edu and they will not get an exchange mailbox. When a student claims the account, the account claim workflow will assign two roles, gmail and student in the IDM, the IDM will directly provision the Google account when the gmail role is set.

People Database, UDB

The people database was populated with data from the old plus system. (The plus system provided SIS, FRS, etc. before Banner was installed in 2007.) There are quite a few applications that still use it. Part

of the migration to Banner included the development of a set of tools to nightly copy data from Banner to the People database to keep these applications running.

The User database, or UDB, managed users before we moved to the current IDM in 2015. Unfortunately, the UDB is still used for a couple of reports.

De-provisioning

Currently, de-provisioning is a manual process. Various reports are gathered from help desk tickets, Banner data (via Cognos), and the old UDB. The picture is not quite perfect, but is used to disable and remove accounts.

Re-Provisioning Returning Users

This has proven to be a difficult problem. As a matter of policy, the user is only allowed to run account claim one time. Name, CWID, and birth-date are good enough for a new user, but an existing user may have a considerable amount of data in Mines systems.

Currently, the IDM is only provisioning new users. If a user leaves and then returns, the help desk must manually turn the account back on. At this point, no effort has been made to configure the IDM to automatically re-enable the account for a returning user.

Benefits and Drawbacks

This system allows for a number of real time changes from Banner to any of the connected systems. Real time creation of various accounts and quick password changes to any system except Luminis, which has a 5 minute delay for a password change.

Convenient administration interface that allows many facets of the user to be modified by the IAM staff.

Unfortunately, there is no automated audit of users. The IDM communicates with Active Directory and Banner via SOAP and SPML, meaning there is no way to access all of the records to compare them to policy.

Due to various difficulties during installation, Mines did not get the system configured to support automated de-provisioning and the automated re-provisioning of returning users.

Currently, the IDM only supports users and related attributes such as common name, surname, display name, user name, home directory, eduPersonAffiliation, and a few others. There is no support for groups or other kind of access control.