Procurement and Contracting Services

Request for Proposals for Identity Access Management (IAM)

RFP L162303

ADDENDUM #1

RFP # L162303
Revised: Due 12/12/22 no later than
2:00 PM, MST

1. Can the University share the IAM team org chart, we don't need names, looking for FTE level, counts, and their brief job description or role on the team?
    - Assistant Director – IAM: Oversees the Access and Integrations teams and projects
    - Access Management team = three information security analysts: Manage the access provisioning and deprovisioning roles, row level security and maintenance for enterprise services through the AccessFlow platform
    - Enterprise Architect – Manager: Over sees the Systems and Integrations team
        i. Oversees – Enterprise Directory system, Grouper, UA id creation systems, SSO platform, MFA
    - System Administrator:
        i. Oversees – Enterprise Directory system, Grouper, UA id creation systems, SSO platform, MFA
    - Systems Programmer:
        i. Oversees – Enterprise Directory system, Grouper, UA id creation systems, SSO platform, MFA
    - Business Analyst: Documentation of practices, analysis, customer service needs

2. Can UofA also share your standard IAM architecture diagram? along with the org structure?
    - Attached
3. In reviewing L162303 Identity Management RFP, it references any work needs to follow what is outlined in the Master Data Management project. Can you provide further clarification?
    - For clarification, what was intended is that there are many new systems that we will need integrate with and understand the hierarchy of data flow between them. A new Master Data management platform is being implemented with BOOMI, Service Now, Access Flow, SABA and others
4. Would the University consider an extension to December 14th, or 16th or ?
    - We will provide an extension to December 12th
5. For our pricing we will need some more information on user counts. How many faculty/staff? How many students? How many alumni? Other affiliates?
    - 3,700 Faculty, 11,000 Staff, 59,500 Student (includes incoming freshman, outgoing seniors), 235,500 Alumni, 20,500 Active other affiliations, 336,500 other affiliations.
    - Student FTE is 47,000

6. Can the University provide a breakdown of its 500,000 identity records? For example, how many alumni, former employees, retirees and contractors access the identity system on a monthly basis?
    - 3,700 Faculty, 11,000 Staff, 59,500 Student, 235,500 Alumni, 20,500 Active other affiliations, 336,500 other affiliations.

7. Out of the 500,000 records, how many unique users access your identity platform every month?
    - We have ~22,000 unique sign-ins to Office 365
    - Last year Shibboleth SSO unique sign-ins per month fluctuated between 85,000 and 98,000

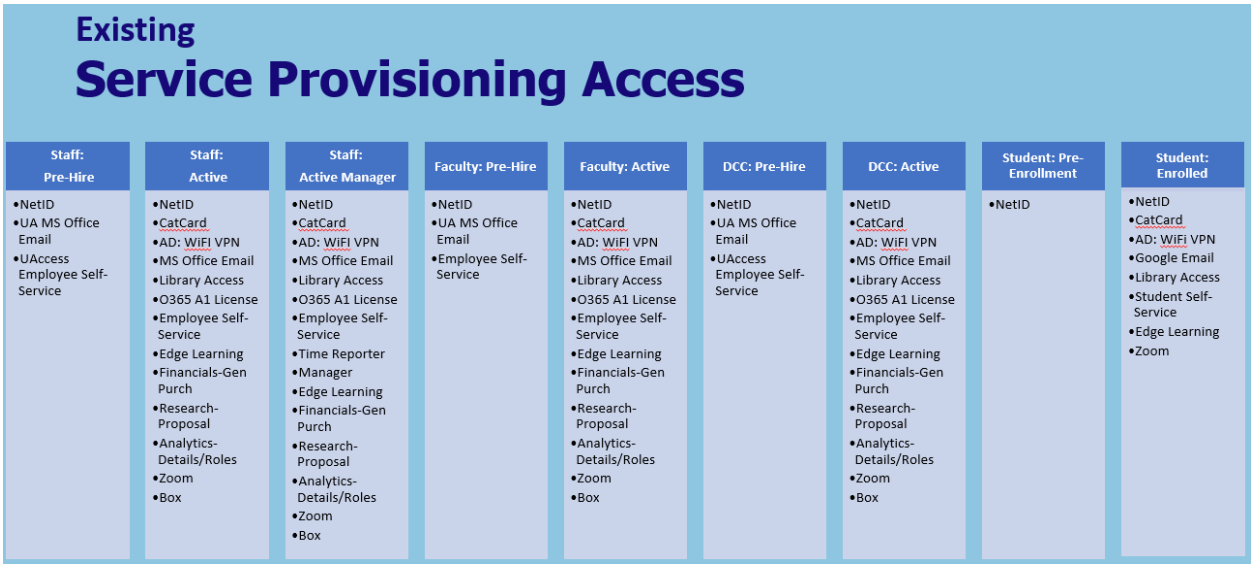
8. Does the scope of the RFP include gathering all regulatory requirements from stakeholders across the University or will this information be provided to the awarded contractor?

- Some information has already been gathered, but there could be additional requirements that would be need to be gathered once policy has been established for all of the items we intend for the solution to provide.

9. Will UofA technical resources be available to support the replication of data from the existing EDS over to the new IdP?
    - Yes
    - EDS is an LDAP directory server (389 Directory Server) which is used as a central attribute store. We have a custom set of ETL scripts to pull data from source systems into EDS nightly.
10. Does the scope of the RFP include reconfiguring the enterprise applications to use the new IAM, or simply to show UofA technical staff how to use the new IAM?
    - Scope would include reconfiguring as well as teaching the staff
11. Can UofA provide the number of unique users accessing the IAM solution on a monthly basis?
    - We have ~22,000 unique sign-ins to Office 365
    - Last year Shibboleth SSO unique sign-ins per month fluctuated between 85,000 and 98,000
12. Can you describe the architecture of the current IAM system (EDS)?
    - EDS is an LDAP directory server (389 Directory Server) which is used as a central attribute store. We have a custom set of ETL scripts to pull data from source systems into EDS nightly.
13. Is the current IAM system (EDS) a home grown or a commercial product?
    - The majority of the big components are home grown. We do use Grouper, Shibboleth for our SSO, Duo for MFA
    - EDS is an LDAP directory server (389 Directory Server) which is used as a central attribute store. We have a custom set of ETL scripts to pull data from source systems into EDS nightly.
14. What user communities would be included within in the IAM system (employees, contractors, student, alumni, etc.) and how many users are in each population?
    - 3,700 Faculty, 11,000 Staff, 59,500 Student, 235,500 Alumni, 20,500 Active other affiliations, 336,500 other affiliations.
    - Not all of these individuals are actively participating in the system
15. What are the authoritative sources for the user communities?
    - Primary authoritative sources are the Student Information System (Peoplesoft Student) and the Employee System (Peoplesoft HCM)
16. How is data consumed from the authoritative sources today?
    - EDS is an LDAP directory server (389 Directory Server) which is used as a central attribute store. We have a custom set of ETL scripts to pull data from source systems into EDS nightly.
    - Additional services will then either pull directly from the same source systems, or pull data from EDS.
17. Do users exist in multiple user communities today? If so, are their accounts separate or correlated?
    -There is some overlap of affiliations. There is only one account per person.
18. How do you currently correlate users from different communities (Name, birthdate, SSN, University ID, personal email, etc.)?
    - There is only a single user identity which can have multiple affiliations.

- The University is beginning a separate Master Data Management initiative with BOOMI to do some correlation work with prospective students and affiliates prior to having a university identity created.

19. What applications for integration should be targeted for Phase 1 (active directory, education platforms, specific app names or types of apps and integrations)?
    - Active Directory/Office 365
    - EDS Refresh Process
        i. Peoplesoft / UAccess Student
        ii. Peoplesoft / UAccess Employee
        iii. LMS / EDGE learning
        iv. Data WarehouseW (Oracle)
    - Box
    - Zoom
    - ServiceNow
20. What user lifecycle events should be included in Phase 1 (Joiner, Mover, Leaver, Emergency Term, Rehire, Attribute Sync, Leave of Absense, User Conversion, etc.)?
    - All of these
21. Should Password Management be included in Phase 1? If so, how is password management handled today?
    - Yes. Password management and account claiming is currently handled with a custom web application. This application provides initial identity proofing to allow the user to select a username, and then set a password. Password resets and recovery are also handled by this web application.
22. Should Access Request be included in Phase 1? If so, please describe current access request processes.
    - Yes. Access request is currently federated and up to the individual service owners. We want to move to a more unified access request solution.
23. Should Certification/Attestations be included in Phase 1? If so, what certifications are performed today?
    - HIPAA, FERPA, Information Security Awareness certifications from our Employee Training System
    - Annual self-service attestation/acceptance of network accepable use policy
    - Period attestation review of group or role membership for audit purposes.
24. Does UofA currently have roles that automatically assign accounts and entitlements? If so, please describe role model.
    - There are some items that are automatically provision once an individual becomes active. Additional role models are requested separately by the department as they are deemed necessary. Investigative work into what other automations could be applied would be important to understand.

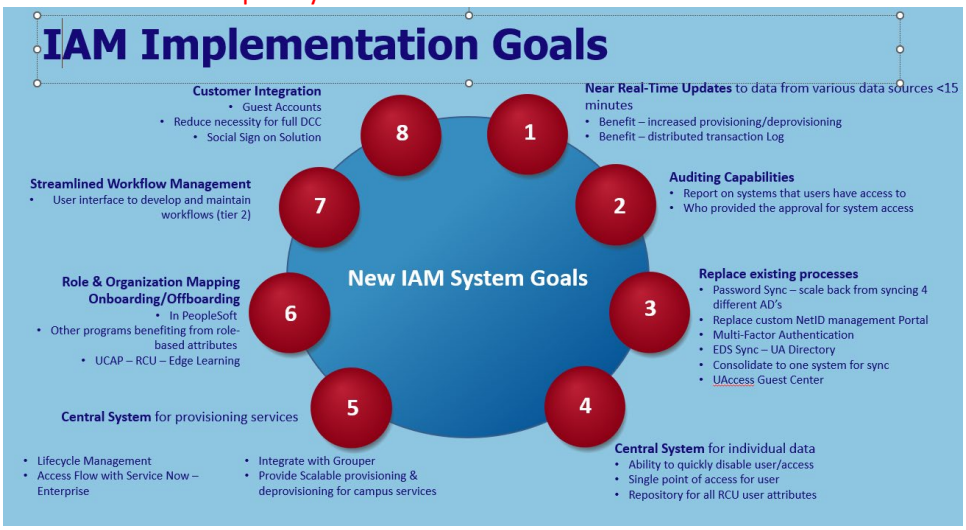
- 

- Some services use group membership as a form of role/entitlements. Some of those groups are automatically provisioned today based on user attributes (for example department number)

25. Does UofA have any training or LMS systems that need to be included
    - Yes. Our Employee EDGE Learning is by SABA. Integrations into this system would need to occur so proper access is only give once certain necessary training is completed based on the access requested.
    - Student LMS is Desire2Learn (D2L). This has a dedicated provisioning workflow in place today and will likely not be part of Phase 1.
26. Should delegated administration be included in Phase 1? If so, please describe current delegated administration functions.
    - Yes
    - The only delegated administrative functions we have currently are for management of Groups. Delegation is not uniform, and is poorly maintained.
27. Does UofA have an Access Management/SSO solution (Ping, Okta, SiteMinder, ADFS, etc.)?
    - We currently use AccessFlow – which is an addon form the Service Now suite. We are looking to potentially replace this in phase 2 or 3 if the new solution provides a better service.
    - UA also utilizes Shibboleth SAML IdP for most SSO integrations
    - We also use native Azure authentication with Password Hash sync for Azure/Office 365 access
28. Does UofA have a multi-factor solution (Ping, Okta, SiteMinder, Azure MFA, etc.)?
    - UA uses DUO for our MFA
    - UA uses Microsoft MFA for accounts managing Azure/Office 365
29. Will users need to connect to the IAM system from the corporate network, private cloud, general internet, or some combination of those?
    - IAM system will need to be accessible to the general public internet as well as internal University networks
30. How do new users currently obtain their initial username and password?
    - Password management and account claiming is currently handled with a custom web application. This application provides initial identity proofing to allow the user to select

a username, and then set a password. Password resets and recovery are also handled by this web application.
    - Students are issued a PIN as part of their admissions letter/email
    - New hires are also issued a PIN

31. Does UofA have a Privileged Access Management (PAM) solution (CyberArk, Delinea, BeyondTrust, Hashicorp)?
    - UA uses a custom Microsoft Identity Management configuration for PAM with Active Directory
32. Should the PAM solution be integrated in Phase 1?
    - This is not part of Phase 1
33. What ticketing or ITSM system does UofA currently use (ServiceNow, Cherwell, Remedy, etc.)?
    - ServiceNow for our Enterprise service. Campus will begin to be integrated into this over the next two years
    - Application development teams use Atlassian JIRA
34. Who will be supporting the IAM solution after go-live? Is UofA considering vendor-supplied managed services as part of this RFP?
    - UA staff will be supporting this after implementation (long term). Support of the product if there are issues or down time will need to be part of the service agreement.
    - Upon first implementation, there will be additioanl support needed for the team as they receive training
35. Is there any decommissioning or migration activities required from the existing IAM system (EDS)?
    - Probably ☹
36. What are the primary pain points of the existing IAM system (EDS)?
    - Lack of auditable access controls. No current system to track and manage what access an individual has across all campus services
    - Speed of attribute updates. Can take days for changes in source systems to be reflected in all downstream systems
    - Overall complexity



37. Are there any firm timelines that are associated with this implementation?
    - There is an expectation of deliverables in the first year (from RFP award) that relate to our phase one. Including Streamlined workflows, replacing existing process, and central system where provisioning for individuals can occur and be audited.

-

38. Are there any major upgrades or changes to major systems planned for 2023 (AD, authoritative source, ITSM, email, etc.)?
    - Financials Modernization
    - Endpoint management project
    - Campus-wide centralization of cloud resources
    -
39. What reporting capabilities are required for Phase 1?
    - General Auditing capabilities around users and their history
    - Usage reports
    - Real time workflow status updates – where an individual is with in the system, regarding what access they have on their journey to being a member of the UA +community
40. Are you looking for a Time and Materials or Fixed-Bid proposal? Would you consider either or both?
    - Will consider either or both
41. Are you looking for a single phase/release of functionality or multi-phase/release?
    - Multi Phase Release
42. Can you describe what training services you're looking for (End user, admin, role owner, application admin, etc.)?
    - Central Admins
    - Application/Service admins
    - System analysts and application owners
    - Departmental Level administrators
43. In 5.1 Project Overview it states, "The vision of the Identity and Access Management modernization is to reduce the number of homegrown applications by implementing a single platform to take on the governance, access and authentication for the University".
    - Are you looking for a converged IAM solution that offers both IGA and Access Management capabilities, or are you open to a best of breed IGA solution that would require a separate vendor solution to address any Access Management needs (SSO, MFA)?
    - Looking for a solution that offers both in some regards. However we are open to exploring both options. We currently have SSO and MFA, but are also looking to have a single platform to reduce the number of services/programs to manage.
44. What is the list of applications that need to be integrated with the IGA and IAM solution? Do these applications support single sign-on, or will they currently require the provisioning of an account into that system? Do these applications exist on-prem or in the cloud?
    - Hundreds of systems will be integrated. Some on-prem, some in cloud, some fully SaaS. Many systems that need to be integrated do not support existing system (Shib) and rely on the AD sync.
    -
45. Are the 500,000 historical identity records stored in MIM or another system? If so, which system?
    - Stored in Enterprise Directory Services (EDS) and a copy in AD/MIM
46. For the various systems that need to be integrated, including ServiceNow, PeopleSoft, Boomi Master Data Management, the current identity repository (assumed to be MIM), Oracle eBusiness, Kuali SaaS, Salesforce, Request for Budget Change system (RBC), eRIB (access to view protocols in Huron System), eDisclosure, Edge Learning, Huron (IRB, COL) which of these integrations need to be functional day one and which can be phased into the solution?

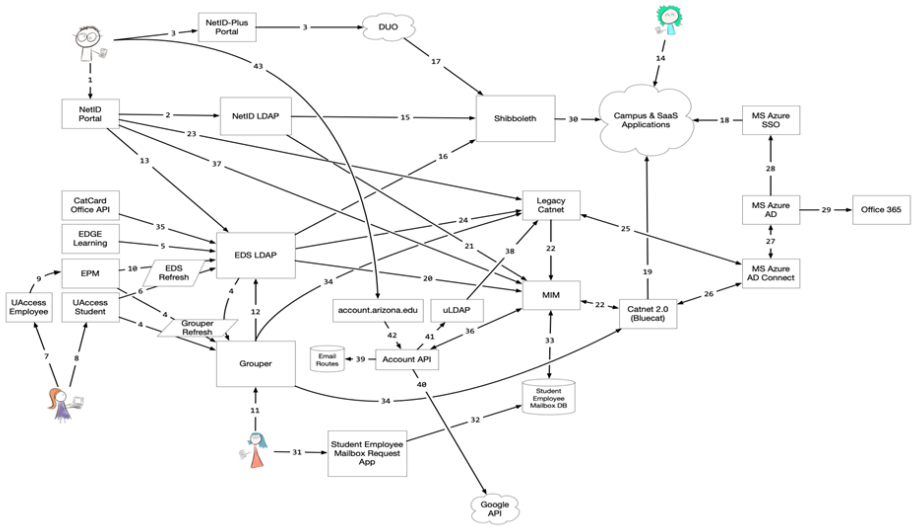
- Very strong preference for a single day / very small window cutover of all services.
- Phase one: PeopleSoft, Service Now,
- Other Phases:

47. For Azure non-gallery applications that require integration, do they have an API available to facilitate communication? (IE: Boomi Master Data Management, Request for Budget Change, eRIB)
    - Varies; should not be assumed
48. Verification from the Q&A session: There are currently approximately 60k total users, between 45k students and 15k faculty and staff.
    - 3,700 Faculty, 11,000 Staff, 59,500 Student, 235,500 Alumni, 20,500 Active other affiliations, 336,500 other affiliations.
49. Can you provide additional documentation or information on your current identity solution, as migration from this solution appears to be part of the scope for this RFP? Or is migration from the current solution not part of this RFP?
    - Our current solution is not one single solution, but rather various pieces that are combined that provide various pieces. Migration of those various pieces would be part of the scope.
50. What documentation is available to further understand the Master Data Management project? Are there other initiatives that this project must be closely aligned with? And if so, what documentation can be provided for these?
    - MDM is currently in implementation and has no artifacts at this time.
51. Verification from the Q&A session: The customer's helpdesk will provide first-level support. Cases will escalate to the vendor as required, but end-users will not be reaching out to the vendor directly.
    - That is correct. Administrative support only
52. What are UoA's expectations for post-implementation support SLAs?
    - There will be a certain level of post implementation support needed as the team is learning the platform and understanding how to continue development.
53. Does UoA have estimated numbers for onboard, offboard and change the volume?
    - About 25,000 / year
54. What system(s) does UoA envision as the source or record for user onboards, offboards, and changes? (IE: PeopleSoft, Workday, ?) For each type (IE: student, employee, faculty, volunteer, alumni, etc.)
    - Student
    - Employee
    - Faculty
    - Volunteer/contractor
        i. Currently all peoplesoft
55. Please provide any details on expectations for training.
    - Being a new solution and the potential for being a replacement with many of our current solutions, training for the UA IAM team will be imperative. Training on how to configure it, functionality, base line development work as needed and key features of the platform.
56. Is the University of Arizona looking to replace your Shiboleth solution with an SSO provider like Okta, Azure SSO or Ping? SSO is a separate sector of the identity management space with a different set of vendors.
    - We are generally content with Shib but are willing to consider alternatives

57. Is the University of Arizona looking for an on prem or cloud solution? Will cloud solutions be given higher weighting considering cloud is now considered industry standard.
    - Looking to cloud solution (SaaS or hosted in public cloud)
58. Is CIAM in scope for this RFP? Considering CIAM is a separate sector of the identity management space with a different set of vendors.
    - Not initially, but we are curious to know what solutions do have a lightweight system as part of their offering. This is something that will be looked at after an initial implementation occurs.
59. Are any of the personas termed as external identities (Alumni, Students, Contractors), or are they all in the same directory?
    - Everybody is in the same directory
60. Please share the approx. number of -
    - Employees – 11,000
    - Faculty – 3,700
    - Students – 59,500
    - Alumni – 235,500
    - Affiliates – 357,000 (Includes all other affiliation types
61. Please provide the list of applications to be considered in phase 1 for IGA (example - these numbers are typically between 10-20)
    - Unknown at this time, pending discussions between IAM/IGA functionality
62. Please share the list of applications that will be onboarded to IGA (Governance, Access Request)
    - Unknown at this time, pending discussions between IAM/IGA functionality
63. Please describe what is MIM's function in the environment?
    - MIM is used to sync from our NetID and EDS systems into Active Directory. It applies business logic to provision AD based resources. We also use MIM as a PAM solution for managing AD and Azure/Office 365 resources.
64. Please share the list of applications that are connected (Connected to Active directory /Other directories)
    - Unknown; pending additional discovery.
65. Please share the number of applications that are disconnected (provisioned manually).
    - At this time there are no disconnected applications that are in scope.
    - This is difficult to ascertain at this time because they are currently being managed by other departments and colleges. two years ago we knew that we have over 300 systems that people were provisioned for. However since they are not centrally managed we do not have an exact number. Also – this could be part of the investigation with each of the departments – what would needed to be included from a auditing perspective.
66. Are all these applications in-scope to be onboarded into IGA?
    - Potentially – this would be over the course of implementation – perhaps not all of the items within the initial scope. Major applications would be in the first rollout of the project. This also allows our team to understand 'how' to onboard departmental applications.
67. What is the HRMS system used for different personas?
    - Peoplesoft Employee / HCM
68. Is there any plan for enhancement to consolidate these systems?
    - NA

69. Do we have the same identifier (SID) used for different user personas? E.g. - In case I am an Alumni and enroll in a new program after a few years, is the same unique identifier (SID) used? what is the process that is followed?
    - There are manual processes in place that should catch these situations and consolidate them. There is also a unique identifier (UAID) as referred to in the RFP.
    - If duplicate person records exist, a merging de-duplication process should be present.
70. Regarding question 4.6 (Attachment A - Section 4) in the RFP - Is there a specific use case or list of applications that need to use SDK?
    - No specific use cases; would depend on what functionality isn't provided by the solution
71. Please share the number of Azure A3 licenses procured. Also, what persona type are these licenses are assigned to?
    - 14,250 Employee A3 licenses. These are applied to most Faculty and Staff
    - 182,000 Student A3 licenses. Applied to all active students.
72. Are there any plans to procure more A3 licenses or upgrade existing licenses?
    - Only if required
73. Please share the count of concurrent users and active users over the period of one year from the total users ~500,000 users mentioned
    - We have ~22,000 unique sign-ins to Office 365
    - Last year Shibboleth SSO unique sign-ins per month fluctuated between 85,000 and 98,000
74. Please confirm the due date for submission of the response for the RFP as there is a discrepancy noted on pages 1 & 5 of the PDF document of the RFP. Is it 11/28 or is it 12/07?
    - We will have the last day to submit a response be December 12th.
75. The schedule of events has different dates than the one mentioned on Page 1.
    -Schedule of events: **12/7**
    -Page 1: **11/28**

    What date should be considered correct for the proposal submission
    - Correct proposal submission date will be December 12th.
76. Does the University have the resources and skills to set-up and maintain the infrastructure required for an Identity solution, based on requirements provided by the vendor?
    - Yes
77. From the implementation timeline diagram shown in Section 5.1, please list the name of each application and its underlying technology e.g., Salesforce, .Net with SQL, etc.) in scope for the Initial Role and Organizational" workstream.
    - See attached diagram for additional information.



-

78. Is the University open to considering a global project delivery model (off-shore resources) without access to production systems or production data, for this IAM modernization initiative?
    - Unknown at this time: would need to consult our general counsel, and export control office

79. Please specify what are the MDM requirements specified in Supplier Profile Questions #3.5. What is the MDM technology platform in use? Is MDM the authoritative source for all user populations.
    - Boomi MDH is the MDM solution. It is not authoritative at this time
80. Please clarify the difference between PeopleSoft generated EMPLID/STUDENTID, CATCARDID, UAID and UA NETID.
    - EMPLID/STUDENTID is an 8 digit number generated from within two separate but synchronized PeopleSoft instances. It is one of the most “known” identifiers for most end users.
    - CATCARDID is an 16 digit ISO number attached to our university ID card. A new number is generated for any lost cards. Within this context it is primarily used as a point in time lookup for card swipes during events.
    - UAID is a 12 digit internally generated unique identifier stored within EDS itself. It is considered the most unchanging identifier for someone, but is largely an internal identifier.
    - UA NETID is essentially a 3 to 16 character, generally human readable, username within our campus IAM system. Constituents choose this username while creating their initial identity. NetID is also the username for their email address. Although discouraged, users can change their netid after the fact.

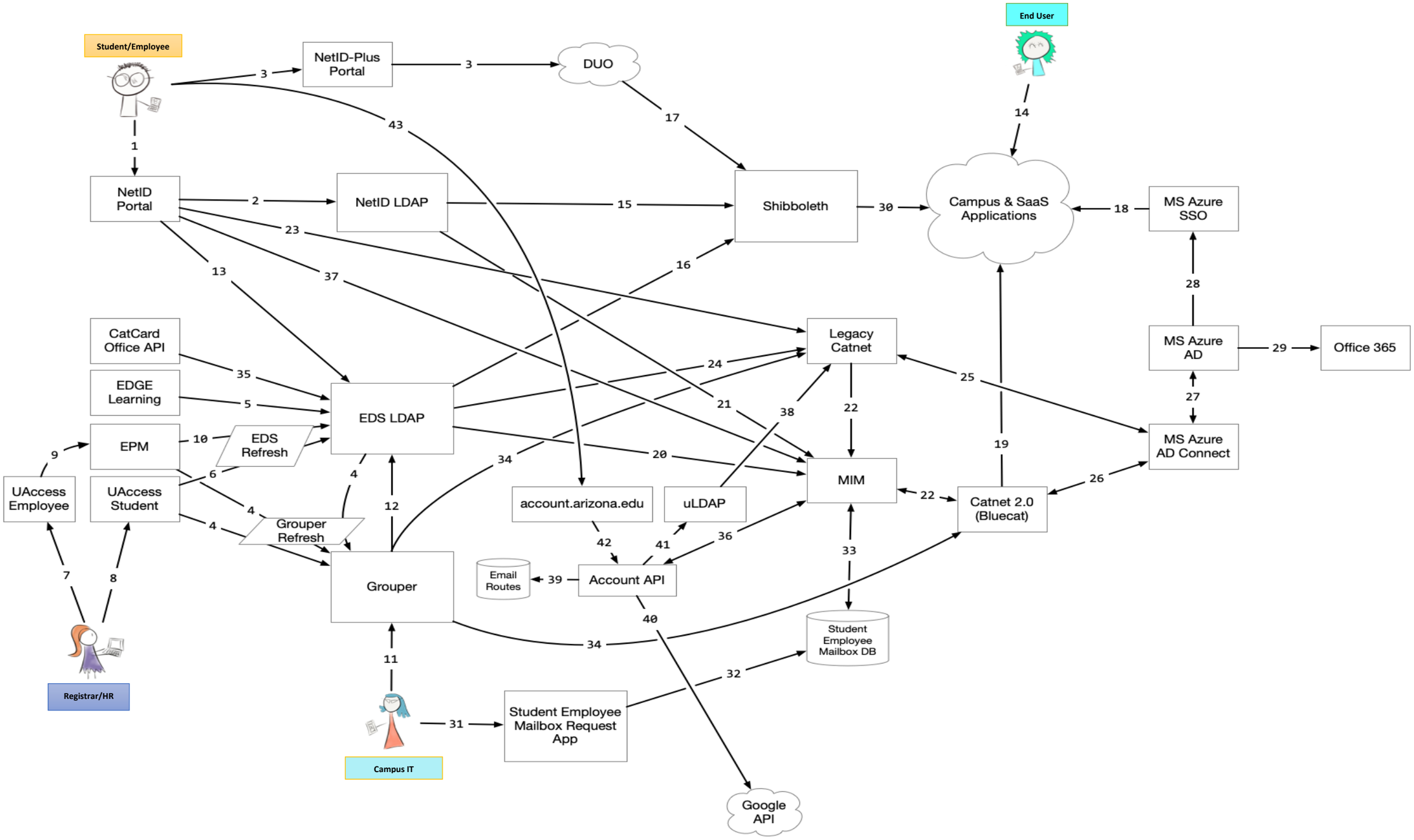
    -
81. Please confirm the list of target applications for the Year 1 implementation with the new Identity solution. Following is the list of target applications for the integration, however, please add any other target systems that may be missing in the list below:

    - AD
    - LDAP

- Google Apps
- Microsoft Office 365
    - PeopleSoft Student
    - PeopleSoft Employee
    - Zoom
    - Box
    - Saba Cloud (Edge Learning)

- There are over 200 authentication consumers that should be considered target applications. The depth and extent of work depends significantly on the capability of the product.

82. The title of the section 5 is labeled as "Password Management" but the requirements specified in 5.1 - 5.6 are around authentication capabilities, please clarify the following:
    1. Is the title of section 5 is an error? This is a password support section
    2. Does the University's current Shibboleth platform meets all the requirements specified between section 5.1 - 5.6. No
    3. Should the vendor responding to section 5 assume to propose a new Authentication solution to replace Shibboleth, please confirm?
        - We do not need to necessarily replace Shibboleth
83. Please confirm if PeopleSoft Campus Solution is authoritative for Student Persona (yes or no)
    - Yes
84. Please confirm if PeopleSoft HCM is authoritative for Employee Persona (yes or no).
    - Yes
85. Please specify the authoritative source of record for Alumni Persona. (e.g., Peoplegrove, Anthology)
    - Currently PeopleSoft Campus Solutions, also pending data sharing agreement with current Alumni System (Lynx)
86. Please specify the authoritative source of record for Affiliate Persona. (e.g., vendors, contractors).
    - Currently PeopleSoft HCM (via the DCC process previously alluded to)
87. Please confirm if the listed integration with OBIEE (Pricing Sheet, Row 22) and the requirement specified in Supplier Profile Questions - Question 3.5 are the same. If not, please clarify what is the intended objected of integration with OBIEE?
    - OBIEE is acting as a SSO consumer.
88. Please clarify the requirement for "SAML, Shibboleth or LDAP integration". Is this in the context of an Authentication solution or an Identity solution?
    - It would depend on the capabilities of the solution whether it's an Authentication or Identity context
89. Please clarify the requirement for "Integration with non-UA systems (content providers and hosted content)". Is this in the context of an Authentication solution or an Identity solution?
    - It would depend on the capabilities of the solution whether it's an Authentication or Identity context


Student/Employee
NetID-Plus Portal
DUO
End User
NetID Portal
NetID LDAP
Shibboleth
Campus & SaaS Applications
MS Azure SSO
CatCard Office API
EDGE Learning
EPM
EDS Refresh
EDS LDAP
Legacy Catnet
MS Azure AD
Office 365
MS Azure AD Connect
UAccess Employee
UAccess Student
Grouper Refresh
Grouper
account.arizona.edu
uLDAP
MIM
Catnet 2.0 (Bluecat)
Email Routes
Account API
Student Employee Mailbox DB
Registrar/HR
Campus IT
Student Employee Mailbox Request App
Google API
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43

1. Student/Employee to NetID Portal
    - Create NetID
    - Set/change NetID password
    - Reset secondary CatNet password
    - Unlock NetID
    - NetID pass codes
    - Manage NetID security questions/secret hint
    - Request and manage Student Employee UAConnect Accounts – CatWorks
2. NetID Portal to NetID LDAP
    - The NetID portal app updates the contents of the NetID LDAP directory in response to user and administrative changes
    - It's done synchronously, the second that somebody selects their NetID and saves a password the NetID portal reaches out to the NetID LDAP directory and stores the data that the user added/changed in NetID LDAP. For example: User changes their password. In response to that, and in real-time, data is stored in NetID LDAP for the NetID Portal
3. Student/Employee to NetID+ Portal to DUO
    - User self-service portal
    - Register for DUO and managed devices
4. Grouper Refresh
    - Pulls from EPM, EDS and UAccess Student
    - EDS to Grouper: Starts after EDS refresh completes. Once a day (12 am to 6 am)
    - EPM to Grouper: Runs in parallel with EDS and UAccess
    - UAccess Student to Grouper: Runs in parallel with EDS and EPM
5. EDGE Learning to EDS LDAP
    - Batch script that updates certifications in EDS
        - Saba Cloud creates a file in their SFTP host
        - Daily process retrieves and processes file (2 am)
        - Daily batch script processes certification expirations
    - Webhook that Saba cloud hits for real-time certification notification
    - Nightly batch process catches missed certifications and processes expirations
6. EDS Refresh - UAccess Student to EDS LDAP
    - Student run starts at 10 pm daily, completed by 1 am
    - Pulls student related data such as Career Program Plan Stacks
7. Registrar/HR to UAccess Employee
    - Workforce Systems makes production changes to UAccess Employee System
    - Business professionals in respective units make direct transaction changes to the employee and student systems
8. Registrar/HR to UAccess Student
    - Registrar's Office processes changes to the main UAccess Student System
    - Business professionals in respective units make direct transaction changes to the employee and student systems
9. UAccess Employee to EPM
    - Data warehouse pull starts at 6 pm
    - Ends no later than 5 am
10. EDS Refresh – HR EPM to EDS Refresh Scripts to EDS
    - EDS Refresh creates affiliations and pushes to EDS
    - Refresh begins at 5 am
    - EDS Refresh scripts pull and process data from data warehouse
    - Takes source data and derives some attributes, either through logic or basic file splitting (employee attributes, affiliations, employee roster, department, discrete attributes, etc.)
11. Campus IT to Grouper
    - Departmental specific group changes
12. Grouper to EDS
    - Group changes reflected in near real-time to EDS
    - Less than 15 minutes
    - PSPNG – Grouper process that continually runs and looks for any membership change
13. NetID Portal to EDS LDAP
    - NetID Portal app updates EDS when a new NetID is chosen
14. End User to Campus & SaaS Applications
    - Interactive flow, end user logs into a service
    - Depending on application configuration, authorization is delegated to an identity provider (Shibboleth, MS Azure, Bluecat)
15. NetID LDAP to Shibboleth
    - Shibboleth uses the NetID LDAP for the password authentication in real-time
16. EDS to Shibboleth
    - Real-time user attribute resolution
17. DUO to Shibboleth
    - Users are directed to DUO for MFA in real-time
18. MS Azure SSO to Campus & SaaS Applications
    - Real-time interactive logins, some campus applications use MS Azure SSO as their identity provider
19. CatNet 2.0 to Campus & SaaS Applications
    - Real-time interactive logins, some campus applications use CatNet 2.0 AD as their identity provider
    - Provides a username and password box
    - After info is entered, it is validated against Bluecat
20. EDS to MIM
    - MIM pulls in data changes from EDS every 30 minutes
    - Runs its transformation and pushes data into the other systems
21. NetID LDAP to MIM
    - MIM pulls in data changes from NetID every 30 minutes
    - Runs its transformation, and pushes data into the other systems

22. MIM ◄► Catnet 2.0 (Bluecat)
    - MIM jobs runs every 30 minutes
    - Runs its transformation and pushes data into the other systems
    - The NetID OU in CatNet 2.0 (Bluecat and Catnip): Two-way import/sync/export
    - The RCU OU in CatNet 2.0 (Bluecat and Catnip): Two-way import/sync/export

    Legacy CatNet to MIM
    - MIM jobs runs every 30 minutes,
    - Runs its transformation and pushes data into the other systems
    - The NetID OU in CatNet (exchange-based information): One-way import/sync
    - The delegated OU structures in CatNet (import mail enabled) service/departmental/shared accounts): One-way import/sync
    - Separate CatNet refresh process (EDS LDAP to Legacy CatNet)
23. Net ID Portal to Legacy CatNet
    - Script runs continuously (monitoring the webservice)
    - Create, rename, delete NetIDs in CatNet
    - Create/update passwords in CatNet
    - Provisions mailbox stubs into CatNet for needed accounts

24. EDS LDAP to Legacy CatNet
    - Script runs daily
    - Updates bio/demo data of users in CatNet
    - Updates email routes for users in CatNet
25. 26. 27.
    Legacy CatNet ◀⟷▶ MS Azure AD Connect
    CatNet 2.0 (Bluecat) ◀⟷▶ MS Azure AD Connect
    MS Azure AD Connect ◀⟷▶ MS Azure AD
    - Azure AD Connect runs the following jobs every 30 minutes:
        - Import/sync from CatNet (25)
        - Import/sync from Bluecat (26)
        - Export Azure AD change back to CatNet and Bluecat (25, 26)
        - Export to Azure AD (27)
        - Reimport from Azure AD (27)
        - Provisions accounts and groups into Azure AD (27)
    - Synchronizes password hash from Bluecat to Azure AD
    - Rules determine if mailbox should be created or modified
28. MS Azure AD to MS Azure SSO
    - Backend Microsoft process
    - User logs in to Azure SSO, pulls its data authority from Azure AD
29. MS Azure AD to Office 365
    - Backend Microsoft sync process inside MS Azure AD and Office 365 that pulls data out of Azure and updates in exchange online
30. Shibboleth to Campus & SaaS Applications
    - End User connects to an SSO integrated application
    - Interactive flow: user logins delegated to identity provider. Campus systems are not pushing to Campus & SaaS Applications
31. Campus IT to Student Employee Mailbox Request App
    - Used by Campus IT for business delegates to request mailboxes for student employees
32. Student Employee Mailbox Request App to Student Employee Mailbox DB
    - App stores a record of the mailbox request in the database
33. Student Employee Mailbox DB ◀⟷▶ MIM
    - Runs every 30 minutes
    - Finds new records in the database
    - Creates new mailboxes for student workers
34. Grouper to CatNet 2.0 (Bluecat)/Grouper to Legacy CatNet
    - Syncs departmental group memberships to CatNet 2.0 (Bluecat) and a subset of course groups
35. CatCard Office API to EDS
    - Every 5 minutes
    - Script that pulls new CatCard numbers into EDS
36. Account API ◀⟷▶ MIM
    - Updates email routes for users
    - Triggered as needed (i.e., affiliation changes)
    - API – talks to the email database, Google API, uLDAP, account.arizona.edu
37. NetID Portal to Active Directory Catnet 2.0, CatNet Legacy
    - Process on MIM server for Catnet 2.0
    - Process on Powershell server for Legacy Catnet
    - NetID Portal provides API to pull password changes
    - Near real-time sync from the NetID service to the AD
38. uLDAP to Legacy CatNet
    - Pulls data for use in automation scripts
39. Account API to Email routes
    - Account API allows other services to update email routes
    - Email routes stored in database
40. Account API to Google API
    - Account API provisions and manages Google accounts
41. Account API to uLDAP
    - Account API provisions and manages uLDAP accounts
42. account.arizona.edu to Account API
    - Facilitates user self-service requests to Account API
    - Allows IT Support to update Account API related systems
43. User to account.arizona.edu
    - User self-service for account provisioning

IAM Thoughts of Future State