REQUEST FOR INFORMATION
No. I-2022-007226-JK

IDENTITY SYSTEM

I. SCHEDULE OF EVENTS

SCHEDULE OF EVENTS:

Issue Date.....November 2, 2021

Due Date and Time.....November 16, 2021 (3:00 pm, PT)

II. ISSUING OFFICE AND CONTACT

ISSUING OFFICE:

The Procurement, Contracts and Materials Management (PCMM) department of Oregon State University (OSU) is the issuing office and is the sole point of contact for this Request for Information. All concerns or questions pertaining to this Request for Information should be appropriately addressed to the individual identified below:

CONTACT PERSON:

Name: Jennifer Koehne
Title: Procurement Contracts Officer

Telephone: (541) 737-7353
E-Mail: jennifer.koehne@oregonstate.edu
Address: Oregon State University
Procurement and Contract Services
644 SW 13th Avenue
Corvallis, Oregon 97333

III. INTRODUCTION

INTRODUCTION:
This is a Request for Information (RFI), issued by Oregon State University (OSU) Procurement, Contracts and Materials Management (PCMM). The purpose of this RFI is to solicit input from potential suppliers for information pertaining to Identity and Access Management solutions.

OREGON STATE UNIVERSITY:
Founded in 1868, Oregon State University is a comprehensive, research-extensive, public university located in Corvallis. Oregon State is one of only two American universities to hold the Land Grant, Sea Grant, Space Grant and Sun Grant designations. Oregon State is also the only Oregon institution to have earned both Carnegie Foundation classifications for Highest Research Activity and Community Engagement, a recognition of the depth and quality of its graduate education and research programs.

Through its centers, institutes, Extension offices and Experiment Stations, Oregon State has a presence in all of Oregon's 36 counties, including its main campus in Corvallis, the Hatfield Marine Sciences Center in Newport and OSU-Cascades Campus in Bend. Oregon State offers undergraduate, master's and doctoral degrees through 11 academic colleges, the Honors College, Graduate School and online Ecampus, enrolling more than 31,000 students from every county in Oregon, every state in the country and more than 110 nations.

IV. REQUIREMENTS

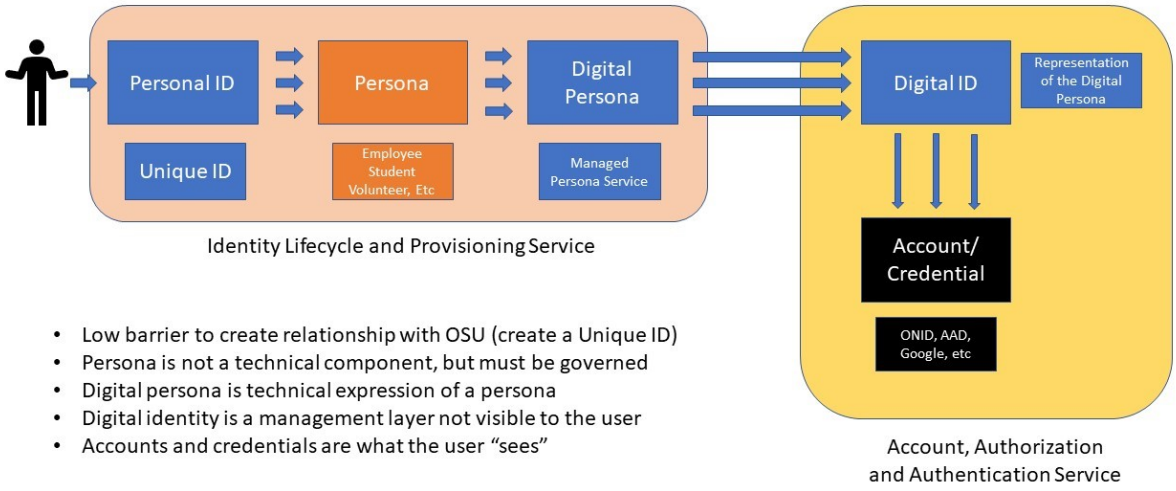
1.0 Purpose of Request for Information

OSU is requesting information to gain feedback from identity and access management suppliers of identity/profile management solutions. OSU is gathering information to better understand the current and future states of identity and access management specifically targeted to institutions of higher education. OSU wants to identify potential solutions that provide better business value, resiliency, simplified operations, lifecycle management, software integrations, and support. This should result in potentially lower Total Cost of Ownership (TCO), providing flexibility for growth and stability for future operations without being locked into one vendor. In order to support the strategic plan of OSU, it is essential that any identity solution OSU entertains, is a solution that will support a wide variety of use cases for providing a single identity for each person who interacts with OSU and allows them to interact with the university in different roles (e.g. parent and student; faculty and volunteer, etc.)

2.0 Background and Current Operation

OSU currently has an identity management solution that is tightly coupled with the role of the individual as either an employee and/or staff member. The identities that it creates are used to onboard employees into centralized and decentralized systems across the university. OSU ideally would like to replace this identity management solution with a modern and more supportable solution, presumably cloud-based or Software as a Service, that decouples the direct tie between the identity and the role of registered student and/or current employee. OSU has a need for a much more flexible identity solution that encompasses more roles and use cases including the ability to have identities for loosely affiliated members of the community such as parents, vendors, guests, volunteers and others.

The approach OSU wants to take to identity is envisioned in this graphic:



Identity Lifecycle and Provisioning Service

- Low barrier to create relationship with OSU (create a Unique ID)
- Persona is not a technical component, but must be governed
- Digital persona is technical expression of a persona
- Digital identity is a management layer not visible to the user
- Accounts and credentials are what the user "sees"

Account, Authorization and Authentication Service

3.0 Supplier Response

General

Please answer General Questions (§ 3.1), Consulting, Training, and Other Services (§ 3.3), and Fees (§ 3.4) as fully as possible. For Features (§ 3.2), answers are optional: if you do not have a solution to the feature (e.g. you provide a CIAM product that does not do provisioning), please answer questions as appropriate to your product features.

OSU is interested in obtaining additional information on any products that may meet our needs and are not limiting ourselves to a combined suite.

Product Information

Please provide information regarding your solution below. If you have other information you would like to share that pertains to your solution that was not mentioned in this document, feel free to provide it in your response.

3.1 General Questions

Please answer the following questions.

I. Introduce your organization.
II. Identify contact(s) for follow-up questions concerning this information and the products and services you offer.
III. List any relevant websites for your company and its products including support, training, and consulting.
IV. Describe your product(s) and services strategy, including markets served. How long has your company been providing these types of products and services? Does your organization serve the higher educational community?
V. Identify or describe your top three customers and provide a paragraph describing the relevant products they use. OSU is particularly interested in your higher education customers; describe your company's experience with higher education customers of a comparable size or government customers of comparable size and complexity, including experience working with federally-regulated research spaces to meet security requirements.
VI. Describe your development roadmap over the next three years. Where do you see your organization from a products and services standpoint five years from now?
    A. How and how often do you work to understand user needs to iteratively improve your products and services?
    B. What is your release schedule and how are major releases coordinated with customers?
VII. Describe if your solution is a locally hosted solution or a cloud/software as a service solution (SaaS).
    A. For installations that require local hosting,
    1. What platforms are supported or required?
    2. Are there roadmap plans for cloud/SaaS in the future? Please provide your product roadmap and any available details for migration.
    B. For cloud or SaaS services,
    1. What options are available for providers?
    2. Describe the location of your data centers and/or platform provider. Please confirm whether all persisted data is kept within the United States.
    C. For products that can be installed either locally or cloud/SaaS, what differences exist in functionality between versions?
VIII. Describe your application status/availability monitoring and auditing capabilities. For SaaS and cloud offerings, what SLAs are available?

A. What external systems do you support for logging, monitoring and auditing?
B. What are your patching and maintenance philosophies?
1. For SaaS or cloud offerings, what are your maintenance windows and what facilities and timeframes are available for us to test? Do your customers have input over when changes are performed to best fit your customer's business cycle?
2. For local installations, what is your support and maintenance lifecycle?

IX. Describe availability of administrative APIs that are available to automate or to build custom interfaces for functionality in Features (§ 3.2) below.
A. What protocols and service types do you support (e.g., REST, SOAP)?
B. What authentication and authorization options are there for any APIs offered and does your product support standards such as SAML, OAuth, and OIDC (OpenID Connect)?

X. OSU is committed to ensuring that our digital environment is accessible and free from barriers for all members of the university community. Describe your approach to accessibility in your products and related services.
A. Do your products and/or services conform to the W3C Web Content Accessibility Guidelines, version 2.1 ("WCAG 2.1") at the conformance levels A and AA, and Section 508?
B. Has the product been tested with assistive technologies (AT)? If so, which AT were used? Who did the testing? What was the testing methodology? What were the results?
C. How is accessibility built into your quality assurance workflow? If you roll out upgrades of the product, how do you assure that upgrades will not break accessibility?
D. Are there known accessibility issues with your products or tools? If so, what are they? What are the work-arounds for users of assistive technology? What is the plan to address these issues?
E. How should accessibility barriers be communicated to you and how does your company respond to such issues?

3.2 Features

As noted above, answer only the questions that pertain to your product or products. Describe how your product or suite would address the features noted below. If a suite, highlight the specific products required from your portfolio and describe how they interact to meet the described business need.

3.2.1 Identity Onboarding

I. Identity Profile Creation
A. Registration: Describe the various workflows available for user registration. In particular, address how your solution would enable the following user registration flows:
1. Self-registration using external (federated) and social login
2. Self-registration and local account creation
3. Self-registration via invitation from central or delegated administrator
4. Conscripted registration by central or delegated administrator with subsequent account claim by individual
B. Deduplication: Describe how your solution can help the user avoid creating duplicate accounts. Describe any clues or workflows in the registration process that would let the user know that they have an existing account.
C. Invitation: Describe how a resource owner could invite a user to access a resource, thereby establishing an authorization to use that resource in addition to inviting the user to self-register.
D. Identity Proofing: Describe the workflows available for establishing proof of the user's identity during the registration process. If a strong identity proofing is required (e.g. photo ID verification or presentation of documents), how would your solution accommodate that?

1. Describe how your product will enable the customer to implement identity proofing as proposed by the US Federal Government in NIST Special Publication 800-63-3A (NIST SP 800-63).
2. Describe how your product will enable the customer to interoperate internationally using the REFEDS Assurance Framework.

E. Account Validation: Describe the controls your solution provides to prevent fraudulent account creation or recovery, either by automated/scripted attack or by malicious users.

F. Unique Identifier: Describe the controls available for creating a unique identifier for each identity.

II. Profile Maintenance

A. Levels of Registration: Describe the ability to track users during the registration process, including:

1. Anonymous visitors
2. Light registration with basic information
3. Full registration with more complete information
4. Full engagement (e.g. registered as a student or hired as an employee)

B. Progressive Profiling: Describe the process by which a user might start with a lightweight registration (for example, collecting only name and email address) and then be prompted for additional information in order to grow their relationship with the customer as they gain deeper affiliation. Describe the mechanisms by which a move from light registration to full registration can be initiated, and by whom.

C. Data Access: Describe how profile information can be made available to other systems and processes in a real-time, queryable format. Describe any event-based integrations that are available when a meaningful event takes place regarding a user's profile (e.g. new registration, update, move from light to full registration, etc.).

1. Consent and GDPR “right to access”: Describe how your platform addresses GDPR's "right to access". How would a user be able to see what has accessed this data and manage authorizations for systems that have or could access the data?

D. Notification Service: Describe how your platform enables users to manage their notification preferences (for example, email, text, in-line) and notifying users about unusual activities with their account.

III. Account Management

A. Account Recovery: Describe the capabilities for self-service password reset and self-service account recovery. Also, describe any functionality you have for providing strong identity proofing during password reset or account recovery.

1. What social or external options are available to outsource this?

B. Account Linking: Describe how the platform could be used to link multiple accounts (external, social, one or more local) to a single identity.

C. Account Merging: When a user discovers they have accidentally created multiple profiles and multiple accounts (locally credentialed or not), what process is available for the user to self-correct, and how are services attached to accounts handled? What process is available to administrators?

1. How does the system manage resolving multiple identities proofed at different Identity Assurance Levels? Specifically address authenticator binding as discussed in NISP SP 800-63-3 Section 6.
2. Does the system have the ability to step-up Authentication Assurance as high as possible when merging?

D. Account Creation: Can users choose between leveraging an external or social account and creating a local credential? If they choose an external account, do they have an opportunity to create a local credential later if they want one or it is required by policy for an application?

IV. Account Identifier: Describe the controls available for creating a unique account identifier (username). Can they be user specified? Can they be generated from an algorithm? Is history maintained to prevent account identifier reuse?

V. Administrative Deduplication/Merging and Splitting

A. Matching: Describe how the software recognizes that two identity records may represent the same person. Describe the back-end technologies and processes as well as the experience for the end user and system administrator.

B. Merging and Splitting: Describe the processes available to merge accounts if more than one account is found to represent the same person. Can a previously merged set of accounts be split later?

VI. Login/Single Sign On (SSO)

A. Restricting Identity Providers: Describe how the customer can set policy to determine which services allow the use of un-vetted identity providers and which do not.

B. Blocking Compromised Accounts: Describe the process by which the customer would block authentication for a user whose external or social account is known to be compromised.

C. MFA: Describe how the platform could be configured to step up to multi-factor authentication (your own or someone else's) based on environmental or risk factors such as a change in location, a new browser, or other hallmarks of possible risk.

D. Consent: Describe how the platform can inform users of what data is being sent to Service Providers, and allow, in some cases, users to edit or remove release of data (withholding, redacting or changing). This functionality must be able to support:

1. Understanding what is required for application functionality and alerting users that an application will not function without appropriate data with a meaningful message.
2. Applications that cannot be turned off (administratively required) and display to the user what attributes are sent, but do not give an option to redact or withhold.

E. Account Login Activity: Describe the types of login activity information the platform logs for users and how it can be accessed and displayed.

3.2.2 Provisioning and Deprovisioning

I. Provisioning and Deprovisioning

A. Connectors: Provide a list of systems to which the platform can provision/deprovision. If there are different cost tiers for different connector types, identify the connectors that are not included in the base product. What connector frameworks and languages do you support for writing connectors?

B. Role- and Attribute-based Access Policies: Describe how the platform can provision and deprovision services dynamically based on data about a person such as a set of roles or affiliations. Also, speak to how this capability would work in a higher education setting, where people frequently occupy multiple roles.

C. Request-based Access Policies: Describe how the platform can support the ability for a user to request access to a resource, and for that request to be routed through a customer-defined workflow for approval.

1. Describe how access policies can include precursor conditions that must be met in addition to approval workflows. For example, access to a system may require that the user be an employee in good standing and have completed IT security training in the last year.

D. Rule-based Access Policies: Describe how the platform could be used to create a role or profile that, when coupled with a parameter, defines a specific set of permissions. For example, a manager (role) within a particular department (parameter) should have a defined set of rights that are scoped only to that department.

E. Attestation: Describe how the platform can be used to trigger an attestation or certification workflow that requires a user or administrator to periodically re-certify that access is still needed, and for that recertification process to trigger an approval workflow.

F. Auditing and Compliance Reporting: Describe how the platform can be used to produce data or reports over time that demonstrate the extent to which users that are provisioned within the system meet the requirements defined by access policies that have been defined within the platform.
G. Rogue Detection and Analysis: Please include any capabilities for bi-directional analysis or rogue detection in provisioned systems.
H. Segregation of Duties: Describe the process by which the platform can prevent a user from obtaining a set of privileges that have been marked as in conflict with other privileges the user has been granted (segregation of duties). Describe the user experience and workflow available (e.g. deny, notify, trigger approval workflow, etc.).

II. Delegated Administration

A. Administration of the System: Describe how the platform can be used to enable delegated administration of users and resources. In particular, address how the following scenarios could be achieved in a distributed, decentralized environment.
1. Distributed IT units defining locally significant roles or groups, assign users to those roles/groups and use those role/groups in access policy decisions, including the ability to invite users to administer roles.
2. Distributed IT units registering an IT service within the platform and define access policies and request/approval processes that determine which users are allowed to use the service.
3. Distributed IT units requesting user attributes (e.g. demo, job, contact) about a population to be delivered, and routing for approval as necessary.

B. Account Management: Describe how the product can manage:
1. How the platform could be used to establish separate login credentials for different services or roles (application-specific passwords and/or usernames).
2. Accounts that are generated and assigned to individuals (service accounts). In particular, describe the process by which a service account could be generated by a distributed IT unit and assigned to an individual. Also, describe the process by which the account is removed when the individual is no longer active.
3. Accounts that are accessed by more than one individual (shared accounts). Can the platform track the individuals with access to the shared account or broker authentication to the shared account? Are there automated password reset or 'break glass' processes available to support improved security for shared accounts?
4. Accounts that are assigned to an individual in a role (role accounts), perhaps even moved between individuals on a daily or weekly basis. Can the platform track what individual had access at which time and broker access to passwords? Can this integrate to role management? Examples might include "receptionist" or "director" accounts that are handed off over time.
5. Accounts associated with non-person entities. Examples might include software agents, machine-to-machine communication, or process automation. Also, define how these non-person accounts can be associated with a responsible/accountable person or group.

III. Consent Based Attribute Release

A. Transparency of Data Usage: Describe how the platform can be used to communicate to the user the data that is being released to a particular application. Describe any controls the platform provides in allowing the user to withhold consent to release data to applications.
B. Organizational Privacy Policy: Describe how we could incorporate references to our organizational privacy policies into the user experiences associated with the platform.
C. Granular Consent: Describe the granularity with which users can express consent and privacy information in the platform. Is it based on classes of information, or can users control the release of each specific data element? What other controls are provided for users to express and manage their privacy preferences?

D. GDPR “right to access”: Describe how the platform addresses GDPR's "right to access". How can a user be able to see the information that the customer holds about them, and what capabilities they have within the platform to alert the customer about data that is erroneous?
E. GDPR “right to be forgotten”: Describe how the platform addresses GDPR's "right to be forgotten". To what extent can a user remove themselves from the system, and what organizational controls can the customer apply to ensure that required records are retained?

IV. Role/Affiliation Catalog

A. Describe what features your system has for identifying and building roles.
B. Describe what features your system has for maintaining roles through their lifecycle.
C. Describe how your system can use data in an external system of record (student or employee system) to automate role assignment and removal.
D. Describe how your system can enable delegated administrators to create new roles and assign them to individuals.
E. Describe how delegated administrators could define workflow and approval processes and drive role assignment based on external data sources.

II. Platform Management

A. Describe the skillsets required for customer employees to support and maintain the platform. Examples include: What is required to build and maintain roles? To administer the platform? To customize workflows? Are specific programming languages required?

3.3 Consulting, Training, and Other Services

I. Does your organization provide technical consulting? Please list the options for those services.

A. Do you have preferred partners, or integration vendors that you recommend working with?

II. Does your organization offer training services? Please list the options for those services.
III. Please list other products and services not specifically identified in this RFI.

3.4 Fees

I. Please describe your pricing and licensing models for education. We are also interested in a model showing five-year life cycles. It should include all upgrade, maintenance and support for those periods.
II. Describe the fee structure for any services you listed in the Consulting, Training, Other Products and Services sections of this RFI.

3.5 Support

I. Describe your support structure and average system uptime. Please provide an example of your typical service level agreement.
II. Does your organization provide technical and help desk support for your products or services? Please list the options for those services including hours and expertise level of after-hours support.
III. For cloud or SaaS offerings, please provide us with an example of a typical service level agreement for your products represented here.
IV. Describe your ongoing maintenance and system testing procedures.
V. Describe your support processes if it is determined to migrate to another organization's product or service.

V. SUBMITTALS

Respondents are requested to submit the following:

- Submit one (1) electronic copy of your response via email that includes the following—
  - Written response addressing §3.0, Supplier Response;
  - Marketing material or brochures of goods or services referenced in the Supplier Response;
  - Examples of work and materials from similar projects as applicable.

To be considered, responses to this RFI must be received no later than the due date and time indicated in the Schedule of Events. Responses must be emailed to the contact person identified in Section II of this RFI.

Information gathered in this process could potentially be incorporated in an Invitation to Bid (ITB) or Request for Proposal (RFP). **Any resulting RFP or ITB will be openly competitive and therefore responses should not be exclusive or restrict competition. This RFI does not obligate OSU to issue an RFP or ITB nor to include information submitted by respondents.**

A contract will not be issued directly from this RFI, nor will issuance or acceptance of submittals or subsequent conversations bind OSU into any type of contractual obligation or relationship.