Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

REQUEST FOR PROPOSALS # 2024-067
Credential Management Solution
RESPONSE ADDENDUM #1
May 2, 2024

CLARIFICATION

Submission Due date is modified to May 9, 2024 on or before 11:59 pm EST.

QUESTIONS

Q1: Could you confirm whether the solution should incorporate AES-256 encryption for data at rest and TLS 1.3 for data in transit, considering the extensive handling of sensitive data across campuses? Additionally, for compliance with regulations such as SOC 2 or GDPR, is the system expected to feature configurable data retention settings and detailed audit trails that capture access and modification events in real-time? This would align with best practices for securing access to programmatic secrets and other sensitive credentials.

A1: Acceptable encryption standards such as AES-256 and TLS 1.3 are required. Configurable data retention settings are not required, but audit logging is required.

Q2: Could the university specify if there is a projected timeline or phased approach for expanding the user base from the initial 300 to the full 5,611, and are there specific triggers, such as enrollment thresholds or administrative milestones, that would initiate each phase of this scale-up? How does the university foresee integrating incremental increases in user licenses into the existing system architecture, particularly in terms of scalability and performance optimization?

A2: At this time there is not a planned projection for growth to the full knowledge worker level of 5,611. Many factors are involved with such as cost/funding for the solution, need/demand and acceptance rates. We would expect that the solution will provide tiered levels of administration to accommodate incremental growth.

Q3: Could the university clarify if the preference is for a linear scalability model for the tiered user licensing or if specific tier thresholds envisioned include significant jumps in user counts? How does the university anticipate these thresholds impacting the required levels of service and support? Are there any specific performance benchmarks or service level agreements (SLAs) that should be met as user tiers increase?

A3: If specific tier thresholds are available that may provide discounts, that may be helpful. Otherwise, linear scalability would work. The same level of support and reliability is expected at any license count, but we can review.

Q4: Could the university specify which primary systems, such as Student Information Systems (SIS) or Learning Management Systems (LMS), the credential management solution needs to integrate with? Are there preferred protocols or APIs, like REST or SOAP, that the university expects the solution to support for these integrations? Are there any unique security or data synchronization challenges associated with these integrations that should be considered in the solution design?

Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

A4: The solution does not need to integrate with SIS or LMS systems. Support for a REST API would be ideal, others can be reviewed.

Q5: Could the university specify if specific types of user authentication methods are required to enhance security while maintaining user friendliness? For instance, is there a preference for multi-factor authentication methods that combine something the user knows (like a password) with something the user has (such as a hardware token or a mobile app)? Are there any considerations for adaptive authentication mechanisms that adjust security measures based on user behavior and access location?

A5: Multifactor authentication is required. Abilility to integrate with both a mobile app and a hardware device is preferable so that either method may be used. Currently, Cisco DUO is used in the UMS, so it is preferred to have support for it in the supported solution alongside alternatives.

Q6: Could the university clarify whether the credential management solution is expected to include dedicated mobile app support for both iOS and Android platforms, thereby enhancing reliability and user-friendliness? Or would a mobile-responsive web interface be sufficient to meet the university's needs? Are there any specific security features or accessibility standards that need to be integrated into the mobile solution to ensure comprehensive user support across all mobile devices?

A6: Native mobileications for common mobile platforms is preferred

Accessability requirements are covered in Appendix I. "Your WCAG 2.1 level AA compliance report, as reported in VPAT 2.4 WCAG applies to mobile applications"

Q7: Could the university specify if the credential management solution must offer API access for integration with third-party developers? Additionally, are there specific security protocols, such as OAuth 2.0 or OpenID Connect, that must be supported by these APIs to ensure secure data exchange and authentication practices?

A7: API Access is only anticipated to be needed by a subset of UMS users, and used as part of automating some workflows. Third party integrations are not anticipated at this time, but any support may add value. No specific security protocols are required at this time, but please include any information on support for them in the proposal.

Q8: Could the university provide further details on whether the credential management solution should include granular permission settings to manage viewing, editing, or sharing of credentials? Specifically, should these permissions be configurable at both departmental and individual user levels to enhance control over sensitive information? Additionally, is there a requirement for auditing capabilities to track changes and access to shared credentials?

A8: Granular permisoons for controlledion is preffered, at a departmental(group) and individual. Audit capability is required.

Q9: Could the university clarify if there is a requirement for the credential management solution to support extensive customization of user roles and permissions? Are there specific administrative

levels and responsibilities across different campuses that must be accommodated, and how detailed should these permission settings be to ensure both security and flexibility in access control?

A9: In general, the more granularityions that are available in the solution, the better as long as management does not become overly complex. From an administrative roles perspective, it will be helpful to have limited roles available for help desk staff for simple user provisioning and visibility.

Q10: Could the university specify whether the credential management solution needs to include real-time monitoring of user activities and an automated alert system for detecting and notifying unauthorized access attempts or other security breaches? What level of detail and immediacy is required in the alert notifications to ensure effective incident response?

A10: This functionality would add value to the solution, but is not required.

Q11: Could the university specify if the credential management solution should support a multi-tenant architecture, enabling each campus or department to independently manage its credentials while still allowing for centralized oversight? What are the specific requirements for data isolation and cross-campus data access within this architecture?

A11: Separate instances do not need to be set up per campus. However departmental managing of credentials is important.

Q12: Could the university clarify if the credential management solution is required to feature comprehensive historical tracking and version control for all credentials? Should this include the ability for administrators to review and revert changes to any credential to previous states, and are there specific audit requirements related to tracking the history of credential modifications?

A12: Historical tracking and revision control for credentials functionality would be of interest, but is not required functionality.

Q13: Our current Intelligent Credential Management System offers a range of additional features that could potentially enhance operational efficiencies and insights. Would The university be interested in exploring these supplementary functionalities, if so, may we include these features in our proposal by adding an "additional features" section?

A13: Additional features are welcome as they might be of interest to us. Evaluation will be made based on criteria provided.