



RFP #881609 Q&A

Question 1: Section 2 Scope of Work on RFP pages 9 to 10 presents two main categories: account claims and identity verification. What is the estimated/approximate annual volume for each of those categories? I.e., the annual number of account claims, and the annual number of identity verifications.

Answer:

Account Claims – 30,000

Identity Verification – 20,000

Question 2: Does MSU envision the Scope of Work on RFP pages 8 to 13 to include an Identity Access Management (IAM) platform, or an integration with MSU's current IAM solution?

Answer: Integration with MSU's current IAM solution

Question 3: The Scope of Work on RFP pages 8 and 9 refers to callers. Is MSU looking to provide a way for people to verify themselves online, without the need to call a service center?

Answer: We are looking to verify in both scenarios.

Question 4: Subsection 6 under Requirements on RFP page 10 refers to a self-service portal. Does MSU intend for the vendor to build this portal?

Answer: Yes, this portal would be supplied by the vendor.

Question 5: Section 2 Scope of Work on RFP pages 9 to 10 presents two main categories: account claims and identity verification. Must a single vendor satisfy requirements under both categories?

Answer: Per section 11: Reservations of the RFP document, the University reserves the right to (k) award multiple, optional-use contracts, or award by of service or good. As such, separate systems may be considered, however, MSU is not obligated to split this award among multiple vendors.

Question 6: Will MSU allow multiple vendors to partner for the RFP response?

We're asking if a prime contractor and a subcontractor can team together and offer an optimal solution for MSU. This would be a single response with a prime contractor managing any subcontractor. The prime contractor would be responsible for the submitted proposal and the resulting contract.

Answer: The University allows the use of subcontractors. A supplier's use of Subcontractors is subject to the terms and conditions listed in section 2.5 in the SaaS Master Service Agreement supplied with this RFP.

Question 7: Subsection 12 on RFP page 10 lists examples of multi-factor ID verification. What does "email/phone verification" mean? Does MSU want a one-time password sent to the email or phone on file? Or is MSU interested in assessing the risk of the phone number and email along with their relationship to the identity?

Answer: This is a TOTP being sent to the phone or email on file.



Question 8: Subsections 12 and 13 on RFP page 10 refer to address verification. Please elaborate further on what this means. Should the solution verify that the identity resides at or is otherwise tied to the address? Or is the address verification requirement meant to ensure a properly formatted address based on United States Postal Service standards?

Answer: This is verification of current or past residency at an address on file.

Question 9: Under the SCOPE OF WORK section, it asks respondents to respond to each section in a written response.

- Does the RFP require the respondents to respond to each paragraph in the Background and Scope of Work sections or only the 3. Implementation Services Framework and 4. Requirements including “Mandatory Minimum Requirements” Sections?

Answer: Please review the table in section 1. Proposal Preparation.

Question 10: ID Verification

- Integration with MSU Systems: The verification system must integrate seamlessly with MSU’s NetID and Affiliate Account management systems to allow secure access to university assets and data.

Can you please clarify or explain what the NetID and Affiliate Account Management Systems are?

Answer: The primary NetID account management system is a MySQL database. The affiliate account management system is SailPoint IdentityIQ, which is backed by an Oracle database. The NetID accounts are also sync’d into SailPoint IdentityIQ.

Question 11: ID Verification

- Integration with MSU Systems: The verification system must integrate seamlessly with MSU’s NetID and Affiliate Account management systems to allow secure access to university assets and data.

What authentication protocols can MSU’s NetID and Affiliate Account systems support when doing identity verification (e.g., SAML, Shibboleth, OIDC, LDAP, Azure AD)?

Answer: MSU’s systems support SAML, Shibboleth, and OIDC.

Question 12: ID Verification

- Integration with MSU Systems: The verification system must integrate seamlessly with MSU’s NetID and Affiliate Account management systems to allow secure access to university assets and data.

What other systems or authentication providers are in place now or will be in place? For example, Okta, Ping, or Auth0?

Answer: Okta is MSU’s IdP.



Question 13: ID Verification

- Integration with MSU Systems: The verification system must integrate seamlessly with MSU's NetID and Affiliate Account management systems to allow secure access to university assets and data.

Does MSU provide APIs, federation data, or configuration documentation that allow integration with a trusted identity verification service?

Answer: MSU can provide API support to allow integration with a trusted identity verification service.

Question 14: ID Verification

- Integration with MSU Systems: The verification system must integrate seamlessly with MSU's NetID and Affiliate Account management systems to allow secure access to university assets and data.

What user attributes (e.g., NetID, Name, Address, Phone Number) can be released or asserted by these systems during the authentication flow?

Answer: This will vary by account type, since MSU does not collect the same data attributes for all identity types. In general: NetID, name, date of birth, and personal email address can be released. Subsets of MSU's identities can also include: home address, work address, home phone, work phone, student/employee identification number, legal sex, and SSN.

Question 15: ID Verification

- Integration with MSU Systems: The verification system must integrate seamlessly with MSU's NetID and Affiliate Account management systems to allow secure access to university assets and data.

How will provisioning, updates, and deprovisioning of NetID and Affiliate accounts be initiated?

Answer: Provisioning, updates, and deprovisioning will take place within MSU's systems. The verification system will integrate with MSU's systems to retrieve data to be able to confidently assert the identity claim.

Question 16: ID Verification

- Integration with MSU Systems: The verification system must integrate seamlessly with MSU's NetID and Affiliate Account management systems to allow secure access to university assets and data.

Are there any differences in how Affiliate accounts must be handled compared to standard NetID accounts (e.g., additional approvals, limited attributes passed, shorter lifecycles)?

Answer: Affiliate accounts will have limited attributes available to be passed to the verification system.



Question 17: Requirements

- Question 3: Solution must allow different levels of identity assurance to be assigned based on account type.

What levels of identity assurance are required?

Answer: NIST IAL1, IAL2, and IAL3.

Question 18: Requirements

- Question 6: Solution must have a self-service portal for users to initiate account claims.

Is this Self-service portal hosted by MSU?

Answer: See Question 4.

Question 19: Requirements

- Question 7: Solution must support integration with MSU's backend systems (Oracle DB, MSSQL DB, MySQL DB, API endpoints) for claim validation.

Please confirm whether MSU relies solely on NetID and Affiliate Account systems for authentication, or if additional identity platforms are in use (e.g., Okta, Ping Identity, ForgeRock, Auth0, or Azure AD). If so, what role do those systems play in authentication workflows?

Answer: MSU relies solely on Okta for authentication. The backend systems mentioned in this requirement are for having a source of truth for the identity verification. Okta also receives the attributes that the backend systems are able to provide, but is considered a secondary source.

Question 20: Requirements

- Question 7: Solution must support integration with MSU's backend systems (Oracle DB, MSSQL DB, MySQL DB, API endpoints) for claim validation.

If additional platforms are used (e.g., Okta, Ping, ForgeRock), can they support federation with via SAML, OIDC, or other standards-based protocols?

Answer: MSU also uses Okta, which supports SAML, Shibboleth, and OIDC.

Question 21: Requirements

- Question 7: Solution must support integration with MSU's backend systems (Oracle DB, MSSQL DB, MySQL DB, API endpoints) for claim validation.

What user attributes (e.g., NetID, Name, Address, Phone Number) can be released or asserted by these systems during the authentication flow?

Answer: See Question 15.



Question 22: Requirements

- Question 18: Solution must provide multiple on-screen language options for end users

What languages are required?

Answer: English is the only individually required language. The number of other supported languages will impact the overall score given to the supplier.

Question 23: Requirements

- Question 26: Solution must have cloud-based or hybrid deployment options.

Can you define or provide clarity on “hybrid deployment options”?

Answer: A hybrid deployment is still primarily cloud-hosted, but also has an on premise agent to act as a gateway between the cloud-hosted application and the on premise database/APIs/applications/etc.

Question 24: Requirements

- Question 26: Solution must have cloud-based or hybrid deployment options.

Please confirm whether MSU requires the solution to be deployed in a cloud-based model, a hybrid model (cloud + on-premises), or if both deployment options must be supported.

Answer: MSU does not require both deployment options to be supported. MSU can support an on-premise agent, but will not be hosting the application locally.

Question 25: Can MSU estimate the **expected annual volume** of identity verification transactions (both remote verification and account claiming)?

Answer: See Question 1.

Question 26: Will **verification events** include password resets, MFA resets, and recovery flows, or only new account claims?

Answer: Verification events include all of the above

Question 27: Does MSU anticipate **seasonal spikes** (e.g., student enrollment, faculty onboarding) that require scalable pricing tiers?

Answer: MSU does have a spike in account claims in April for the students accepted for the Fall term. This is up to triple our average ~2,300 account claims per month. Whether or not this spike requires a scalable pricing tier is up to the supplier.

Question 28: What are the estimated populations for each group listed (students, faculty, staff, alumni, retirees, third-party affiliates)?

Answer: Students – 80,000, faculty/staff – 40,000, alumni – 480,000, retirees – 5,500, third-party/non-employee – 160,000

Question 29: Are these groups **verified at different assurance levels** (per NIST 800-63A), and should pricing reflect that variation?

Answer: The groups are verified at different assurance levels per NIST 800-63A. How much pricing reflects the different requirements is up to the supplier.



Question 30: How many of the service desk identity verifications per year are expected to transition to this automated solution?

Answer: See Question 1.

Question 31: Does MSU expect to use the verification service for **ongoing authentication recovery**, or only for **initial onboarding**?

Answer: MSU expects to use the verification service for both initial onboarding and ongoing authentication recovery.

Question 32: Will MSU require **on-prem or hybrid integration** that affects implementation pricing (e.g., integration to NetID, Oracle DB, or existing IAM platforms)?

Answer: MSU does require integration with our on-premise systems.

Question 33: How many total integrations (e.g., Banner, AD/LDAP, MFA, SSO, HR, SIS) should vendors assume in implementation pricing?

Answer: There are 4 systems that need to be integrated with – a MySQL database, SailPoint IdentityIQ backed by an Oracle database, SAP-HCM, and PeopleSoft Campus Solutions.

Question 34: Should ongoing usage (verification volume) be billed monthly, quarterly, or annually?

Answer: Once a vendor is selected, MSU will work on payment terms for billing usage.

Question 35: Would MSU like separate pricing for **optional components** such as:

- Biometric verification
- Government ID validation
- OCR/document scanning
- Fraud detection and flagging
- Reporting dashboards or analytics API

Answer: Yes, please include separate pricing for optional components such as those listed in this question.

Question 36: Should these (options in Question 35) be quoted as **line-item options** for potential future adoption?

Answer: Yes, please quote them as potential add-ons.

Question 37: Should professional services be priced **per milestone** (planning, integration, UAT, rollout, hypercare), or as a fixed total?

Answer: Please make sure to complete the pricing sheet as indicated in the RFP, page 14. You may also present your pricing as you would normally with your bidding process in your format. Please present professional services pricing as you normally would.

Question 38: Are vendors expected to provide **onsite training**, and if so, for how many MSU administrators or help-desk agents?

Answer: No, onsite training will not be necessary.



Question 39: What level of support coverage does MSU expect (e.g., 24x7 vs. business hours)?

Answer: MSU would like coverage in alignment with our IT Service Desk hours – 7AM-12PM, 7 days a week.

Question 40: Should vendors include **SLA-backed response time pricing** or treat support as included in annual licensing?

Answer: Please provide pricing on both – SLA and General Support.

Question 41: How many accounts (NetID + affiliate) are expected to grow annually over the next 3 years?

Answer: See Question 1 for annual account claims. Over 3 years, this is expected to grow by 90,000.

Question 42: Should vendors include **multi-year pricing** with projected growth and discount tiers?

Answer: Please see the Pricing sheet on page 14. MSU is requesting 3-year pricing.