Identity and Access Management Evaluation Criteria for Software Purchasing

Identity and Access Management Technical Advisory Group

4/18/2014

Evaluating Technology Solutions

The following guide is intended to help application owners and project teams evaluate proposed solutions for their fit with UW System's Identity and Access Management (IAM) technology architecture. The goal is to acquire technology solutions that are easy to integrate, supportable, secure and cost efficient. This guide does not address the evaluation of business functionality but tries to ensure that IAM infrastructure and integration requirements are appropriately considered.

Following are a list of questions along with general guidance for evaluating Request for Information (RFI) or Request for Proposal (RFP) responses and/or Proof of Concept results.

A number has been assigned to each guidance statement indicating the score to apply should analysis and/or the response to an RFP/RFI question match the guidance.

- 9 – In relation to the requirement, the solution is consistent with our current and/or future architecture.
- 3 - In relation to the requirement, the solution is not consistent with our current and/or future architecture, but **can** be accommodated with relatively little effort and/or risk.
- 1- In relation to the requirement, the solution is not consistent with our current and/or future architecture, but **may** be accommodated with significant effort and/or risk.
- 0 - In relation to the requirement, the solution is not consistent with our current and/or future architecture and **may not be able to be accommodated.**

This guide is not intended as a substitute for the engagement of Subject Matter Experts (SME). It is strongly advised that SMEs be involved in the evaluation of technology solutions. SMEs for each category are listed below.

Note that "solution" refers generically to any software application, device, appliance, or contracted service (e.g. hosted email, cloud email, etc.) being considered for acquisition.

Identity and Access Management (IAM)

SME: Identity and Access Management Technical Advisory Group (IAM-TAG)

Tags: [IAM], [IdM]

IAM is composed of two high-level domains, Identity Management (IdM) and Access Management.

An IdM system manages the digital representation of persons, including useful attributes (name, email address, department, photo etc.), permissions (what they are allowed or not allowed to do) and credentials (user id, password, digital certificate).

An Access Management system manages and enforces policies that ensure users only access solution functions and/or data they are authorized for.

Ideally, solutions leave most if not all IAM functions to the enterprise IAM infrastructure, calling on IAM services as needed. Unfortunately, most solutions have not evolved to this point and include their own, often non-standard methods for storing identities, managing identities and providing access.

Any solution that will be used by all or most campus or UW System faculty/staff and/or students will **require** integration with UW System's IdM/IAM infrastructure. More technical or specialized solutions can benefit from IAM integration but the cost to benefit may not be justified. As a general rule, the more potential users of a solution, the more important it is that the solution has good support for integrating with our IAM infrastructure.

Note that some applications still allow or deny access based on the client's IP address. Any solution that uses this method exclusively has no identity management and should be avoided.

IAM 1: Where is the user identity data required by your solution stored?

9: The solution can consume identity data via SAML assertion during the user login process.

3: The solution can leverage identity information stored in a specific, University supported directory server or database view.

1: The solution can be customized to integrate with a supported directory or database view and/or supports directory or database views not included in our infrastructure.

0: The solution has no ability to integrate with an external LDAP or database view and customization would be difficult or impossible.

IAM 2: How does your solution leverage Directory data? Can the solution access data in real-time, as needed or must Directory data be replicated into the local person store? What methods and protocols are supported for querying the Directory?

9: The solution can consume identity data via SAML assertion during the user login process.

3: The solution can query the Directory via a Lightweight Directory Services Protocol query using SSL.

0: Person data must be replicated from the institutional Directory and persisted in a local store, or can only be queried from a directory without the use of SSL.

IAM 3: If a local solution account is required, does the application provide an API that allows for the programmatic provisioning (creation) of user accounts and/or is a connector available for commercial Identity Management Frameworks (e.g. Oracle Identity Manager)?

9: The solution can provision dynamically on first user login, collecting required user information via SAML assertion.

9: The solution provides a web services interface that can receive Service Provisioning Markup Language (SPML) messages.

3: The solution provides a proprietary web services interface that can receive provisioning messages.

3: A commercial connector is available for provisioning accounts.

1: A non-web services based API is available for provisioning accounts.

0: No interface is provided. Local accounts must be manually provisioned via a user interface.

IAM 4: If a local solution account is required, does the application provide an API that allows for the programmatic deprovisioning of user accounts and/or is a connector available for commercial Identity Management Frameworks (e.g. Oracle Identity Manager)?

9: The solution provides the capacity for automated disabling and/or deprovisioning of accounts based on user-defined criteria such as last login date.

9: The solution provides a web services interface that can receive Service Provisioning Markup Language (SPML) messages.

3: The solution provides a proprietary web services interface that can receive deprovisioning messages.

3: A commercial connector is available deprovisioning accounts.

1: A non-web services based API is available for deprovisioning accounts.

0: No interface is provided. Local accounts must be manually deprovisioned via a user interface.

IAM 5: If a local solution account is required, does the application provide an API that allows for the programmatic synchronization of user attributes between the enterprise directory and the local account and/or is a connector available for commercial Identity Management Frameworks (e.g. Oracle Identity Manager)?

9: The application provides a web services interface that can receive Service Provisioning Markup Language (SPML) messages and/or can use a Security Assertion Markup Language (SAML) assertion to synchronize attributes.

3: The solution provides a proprietary web services interface that can receive user attribute messages.

3: A commercial connector is available for synchronizing attributes.

1: A non-web services based API is available for synchronizing attributes.

0: No interface is provided. Local accounts must be manually updated via a user interface.

IAM 6: Can the solution leverage an external security service or repository to make access control decisions? For example allow/deny access to a screen, function or data?

9: The solution can in real-time access an Extensible Access Control Markup (XACML) –based external security decision service.

9: The solution can accept Security Assertion Markup Language assertions for use in making the access decision.

3: The solution can in real-time, via a web service, query a repository (e.g. Directory) to establish whether the user is a member of a group has a role and/or has an attribute which would allow or deny access.

3: The solution can query the Directory via a Lightweight Directory Services Protocol query using SSL.

1: The solution can query the Directory via a Lightweight Directory Services Protocol query with no support for SSL.

0: The solution cannot leverage an external service or repository to make access control decisions.

IAM 7: Can the solution leverage an external authentication service for web user interfaces? Specifically, can it support and Single Sign-on via integration with Shibboleth/SAML by accepting a standards-based assertion from the enterprise web access management (WAM) infrastructure, eliminating the need for a user to login if they have already logged in, or redirect them to the enterprise WAM for authentication?

9: The solution is "pre-integrated" to support SAML V2.

3: The solution includes "authentication interfaces" that support using an external authentication service or can be integrated with an external authentication proxy.

0: No support for external authentication services.

IAM 8: Does the solution support interoperability with SAML2-based Identity Federations?

9: The solution supports interoperability with multiple external Identity Providers and Discovery Services and dynamically publishes and consumes federation metadata (including cryptographic keys) in order to obtain information about federation endpoints.

3: The solution supports interoperability with multiple external Identity Providers that are registered manually to the solution.

0: No support for external authentication services.

IAM 9: Does the solution use standards-based attribute schemas (e.g. eduPerson) for representation of person data within SAML exchanges?

9: The solution natively uses eduPerson schema attributes for consumption of identity data.

3: The solution can be customized to consume eduPerson schema attributes for identity data.

0: No support for eduPerson schema attributes, or eduPerson schema attributes are repurposed for other than their published intent.

IAM 10: Does the solution allow flexibility in assignment of a unique user identifier?

9: The solution natively uses eduPersonPrincipalName or eduPersonTargetedID as a unique identifier.

3: The solution provides the ability to define a unique key based on UW System's unique identifier(s) of choice.

0: No support for eduPersonPrincipalName, eduPersonTargetedID or a UW System unique identifier

IAM 11: Does the solution gracefully handle changes to a unique identifier?

9: The solution gracefully handles changes to a unique identifier that appear in a SAML assertion or other data feed without loss of functionality or data for that user.

3: The solution provides a programmatic interface for updating a user's unique identifier without loss of functionality or data for that user.

0: The solution does not support changes to unique identifiers, or provides only manual methods for handling identifier changes.

IAM 12: Does the solution provide the ability to for UW System to convey user privacy to the application, and does the application mediate display of information appropriately based on this information?

9: The solution provides a means for UW System to designate users as private, and provides a means of restricting display of these users' information to only those people that have a legitimate business need to see their information.

0: The solution does not provide a means for UW System to designate users as private, nor limit the display of their information to those people that have a legitimate business need to see their information

IAM 13: Does the solution's integration with the enterprise WAM support deep linking, the practice of navigating to a page "deep" within an application, thus bypassing the application's and/or the portal's main page?

9: Complete support for deep linking. The user, if already logged in can navigate directly to pages for which they are authorized without logging in again.

0: No or limited support for deep linking, the user is forced to login again, is redirected to the application's proprietary login mechanism or is denied access for which they are authorized.

The analysis necessary to evaluate the solution's access security model will vary widely depending on its architecture, target user population and the data it persists. The following are general questions, but more specific questions should be included as applicable.

IAM 14: Can a user be restricted by both function (create, edit, delete, etc.) and object (i.e. the "things" created and managed by the system, e.g. payroll record, wiki page, document, etc.)? What functions can be restricted?

9: Granular security where each important function **and** object can be explicitly restricted to authorized users.

3: Granular security associated with functions or objects, but not both. Usually, this means functions can be assigned at a granular level, but objects cannot be restricted.

0: Course security where users **must** be granted access to a broad range of functions and/or objects.

IAM 15: Can functions and or access to objects be grouped to create "roles" that can then be assigned to users?

9: Important functions and objects can be grouped into roles for assignment to users.

0: Authorization to act on important functions and/or objects must be individually assigned to users.

IAM 16: Assuming the solution supports "roles", are standard, pre-defined roles included and will these roles support the required business functions?

9: The solution includes pre-defined roles that meet the business requirements (e.g. Administrator, Supervisor, etc.).

3: The solution does not include pre-defined roles.

1: Pre-defined roles do not meet the business requirements (e.g. oftentimes pre-defined roles grant more access than desirable).

IAM 17: Many security models use inheritance to streamline the granting of permissions. If the application uses this model, can permission be explicitly denied on a child function and/or object?

9: Permission to use a function, group of functions, objects and groups of objects can be denied at any point in the authorization tree.

0: Inheritance is absolute and cannot be modified at a point lower than the grant of permission.