HUIT Primary Responsible office: Identity and Access Management (IAM)	**Original Approval Date**: July 5, 2022
Approval Body: Information Security Council	**Effective Date**: August 1, 2022
Version Number: 1.0	**Revision Date**: NA
Version Approval Date: July 5, 2022	**Applicable to**: All applications integrating with HarvardKey
Key Contact: Gretchen Gingo	**Subject Area:** Application Integration, HarvardKey,

HarvardKey Application Integration Policy

Policy Purpose

Deploying applications securely to users in the Harvard community requires integration with Harvard IT infrastructure. The purpose of the Application Integration Policy is to clarify the responsibilities of participants attached to the application to collaborate with HUIT Identity and Access Management (IAM) systems and Service Providers (SPs) towards integrating applications with HarvardKey Authentication and Authorization Services. The policy intends to enable application participants to understand the minimum requirements they need to meet to integrate with HarvardKey Authentication and Authorization services. In addition, it will ensure that all applications integrating with HarvardKey align with HUIT information security standards. Compliance with this policy is not optional.

Who Must Comply

The policy applies to all participants in the application integration process. The policy will go into effect on August 1, 2022. Applications integrating with HarvardKey after this date (including new registrations for existing applications) will need to meet policy requirements in order to integrate. Applications already integrated with HarvardKey will have until January 31, 2023 to bring existing registrations into compliance. The first attestation cycle will take place in Spring 2023.

Overview

The Application Integration Policy Initiative covers the following categories:

Category	Overview
Eligibility to Integrate with HarvardKey	Enables application owners to understand the requirements they need to meet in order to integrate with HarvardKey Authentication and Authorization services.
Standards for Attribute Release	Establishes requirements for single sign-on attribute release, in order to provide ease of use, federation, and awareness relative to the use of personal identity data for authentication, and to maximize the security of identity data while minimizing its misuse or theft.

Application Security Assessment and Standards for Assigning Authorization	Outlines the responsibility of application owners to assess the sensitivity and risk level associated with an application based on Harvard's security policy benchmarks in order to ensure that the authorization approach that is adopted will be sufficient to protect both individuals and the University from material harm. Requires all applications integrated with HarvardKey use an authorization filter in alignment with HarvardKey Affiliation and Assurance tier classifications.
Attestation Requirements	Informs application owners of the commitment they make to participate in regular assessments of their application by HUIT in return for use of the HarvardKey Authentication and Authorization services. Ensures that if an application has undergone any changes, any needed policy adjustments to meet authorization rules can be identified and implemented.
Authentication and Authorization Services Lifecycle Management	Outlines expectations for lifecycle management of authentication and authorization offerings, notification to application owners regarding upgrades or decommissioning of offerings, and responsibilities of application teams to facilitate transition to new offerings.
Roles & Responsibilities	Defines roles and responsibilities of IAM vs. application teams in the integration process.
Consequences of Policy Violation	Outlines the possible consequences if a registered application or individual is found to be in violation of the policy.

Policy Statements

Eligibility to Integrate with HarvardKey

1. To be eligible to register with the HarvardKey Authentication service, an application must support the mission of Harvard University.
2. A benefits-eligible employee of the University and their associated administrative unit or academic department must sponsor the application. Registrations for applications developed, maintained, or owned by students must be sponsored by an administrative unit or academic department that agrees to assume technical ownership of the application upon the student's departure from Harvard.
3. The application must be under the management of Harvard University employees. For applications managed by contingent staff officially contracted by the University or acquired through a third-party with a reputable vendor the contract for the application must be reviewed by the Contract Management Office, a local Harvard procurement team, and/or the Office of the General Counsel.
    a. IAM may request a review if a Harvard department signed a contract without oversight from a local Harvard procurement team, the Contract Management Office, or the Office of the General Counsel in conjunction with the request to register with HarvardKey service.
    b. This review must confirm that the appropriate protections for users and the University are in place before the production registration with HarvardKey is enabled.
4. All applications must use one of the currently supported HarvardKey standard authentication protocols.

5. All applications that integrate with HarvardKey services are expected to comply with relevant Harvard policies and guidelines including but not limited to the Information Security Policy, Accessible Technology Procurement and Development Policy, the General Records Schedule and Harvard's data privacy guiding principles.

Standards for Unique Identifiers

1. It is strongly recommended that applications accept an opaque, unique, immutable identifier such as EPPN, NetID, or UUID to protect users' privacy.
2. Application owners requesting use of HUID or another non-opaque identifier must provide a business justification for consideration of an exception.

Standards for Attribute Release

1. Attributes obtained through authentication are for purposes of authorization, account provisioning, and facilitation of the end user's session and should be deleted or anonymized when no longer needed for service access.
2. Application owners must provide a business justification for the attributes they request. Release of certain attributes requires special approval by IAM. Additionally, the release of certain attributes to vendor-hosted applications requires completion of specific riders along with the contract.
3. Application owners should only request the least-intrusive set of attributes needed and should not retain any extra attributes received.
4. Applications will be eligible for release of attributes based on their authorization approach.
5. The release of all groups that a person is a member of in the authentication response is disallowed. The "memberOf" attribute must be limited to groups contained in specific folders, or to specific groups.
6. Applications using attributes to create a directory browsable by end users of the application must be in alignment with University data privacy guiding principles, directory listing policy and FERPA requirements and honor user privacy by allowing individual users to opt out or acknowledge upon login that this data will be visible.

Application Security Assessment and Standards for Assigning Authorization

1. Application owners are responsible for assessing the data and system risk level associated with their application based on Harvard's security policy benchmarks in order to ensure that the authorization approach adopted will be sufficient to protect both individuals and the University from material harm.
2. All application registrations must include a HarvardKey authorization filter that uses group membership information to restrict application access based on data and system risk level in alignment with HarvardKey Affiliation and Assurance Tier classifications. The tiers ensure proper mapping between user identity and the risk levels associated with the application.
    a. Applications with a higher data or system risk level classification must not grant privileged access to users with lower affiliation and assurance tiers.
    b. Applications can have a more restrictive authorization filter even if data or risk level is low.

3. Use of a bundle or reference group alone is not permitted for application authorization. Applications must use a group designed for authorization, either generic or application-specific.
4. Use of an application authorization filter that includes Alumni reference groups, including a generic application authorization filter that includes Alumni, requires a Terms of Agreement with Alumni Data Governance.
5. Exception process: if an application requires a broader authorization filter than would be implied by the Affiliation and Assurance tiers the application must document how authorization is being handled to limit access to high risk resources.
    a. Exceptions must be approved by the school's security officer as well as the University Chief Information Security and Privacy Officer
6. The application owner is responsible for lifecycle management of local user accounts for their application

Attestation Requirements

1. Application owners are required to review their registration data annually and attest that:
    a. The application associated with the registration is still active and each registration should be retained
    b. The system risk and data levels associated with the application are accurate
    c. The authorization filter in use is appropriate given the system risk and data levels and aligns with Standards for Assigning Authorization
    d. Attributes are being used in accordance with this policy
    e. For applications acquired through a third-party the contract is still in effect and any renewals have been reviewed by a local Harvard procurement team, the Office of Strategic Procurement or the Office of the General Counsel
2. If an application owner cannot attest, they must outline the areas of non-compliance and provide a remediation plan and timeline to bring the registration(s) into compliance

Authentication and Authorization Services Lifecycle Management

1. IAM regularly assesses authentication and authorization service offerings to ensure alignment with industry best practices and may retire a service
    a. IAM will provide at least 12 months' notice before retiring a service.
    b. Application owners must migrate to new offerings within the retirement period.
2. IAM will provide three months' notice before a significant service upgrade unless a shorter window is needed to address a critical vulnerability.
    a. IAM will provide application owners with an opportunity to test the upgrade in a pre-production environment as well as one or more dry runs in production, as needed. Application owners are expected to participate in testing and to notify IAM during the testing window of any issues affecting their service so they can be investigated and resolved in advance of the upgrade.
        i. IAM will test the upgrade against any top 20 HUIT-managed Critical 0 Applications using HarvardKey but not all integrated services

Roles and Responsibilities

Application Owners

1. Complete a preliminary application registration form, enter and maintain data about the application in HKAR, including a current list of contacts with at least one (1) Registration Manager
2. Allow for enough time during their application development cycle for consultation and integration with HarvardKey
    a. Application owners new to HarvardKey should review the HarvardKey Application Integration Services section of the IAM website and then schedule time to consult with the IAM team
3. Provide technical resources to collaborate with the IAM team during the application integration process. (If a vendor is handling the technical configuration, have them identify a technical representative to serve in this role.) Technical resources should:
    a. Become familiar with authentication and authorization practices and supported CAS/SAML protocols
    b. Have the necessary access to configure authentication on the application end
    c. Understand attributes required by the application and determine the unique identifier
    d. Answer questions required to finalize authentication design (e.g., whether the application can handle an encrypted token, whether the application requires a name ID)
4. Configure the protocol-specific components of authentication in the service provider application in consultation with external documentation
5. Manage the lifecycle of SAML SP Signing and Encryption Certificates
    a. Generate signing and encryption certificates with a minimum expiration of three (3) years, consistent with InCommon Federation best-practices. IAM recommends generating long-term self-signed certificates.
    b. Monitor the expiration date of the certificate(s) and submit a request to IAM to replace the certificate a minimum of two weeks in advance of expiration
6. Be a proper steward of attribute data in alignment with the Standards for Attribute Release section of this policy.
7. Direct users to the official HarvardKey credential collector (sign in page) for entering their authentication credentials (e.g., ID and password pair). The user must be redirected to this page and the page must not be presented to the user via web frames or any other method.
8. Secure the application to ensure that only users with a valid assertion are granted access. To secure application access, IAM provides a single assertion upon login and blocks or allows the authentication request based on authorization filters. IAM is not restricting user access beyond initial authentication. Session management is the responsibility of the application.
9. Manage the provisioning of access and revocation of access for their application.
10. Ensure that the application team and third party vendors comply with relevant Harvard policies and guidelines including but not limited to the Information Security Policy, Accessible Technology Procurement and Development Policy, the General Records Schedule and Harvard's data privacy guiding principles.
11. Review the application registration data annually

12. Monitor application availability using a URL that does not require a HarvardKey login. Report unplanned application outages likely to result in significant Service Desk traffic by emailing huit-supportctr@mailman.fas.harvard.edu and iam_help@harvard.edu.
13. Notify IAM of faults or issues (e.g., breach) by emailing iam_help@harvard.edu

IAM

1. Provide and maintain the HarvardKey authentication and authorization service
    a. Routinely update and patch the platform with minor releases and security patches
    b. Monitor service availability and communicate service interruptions or degradation through standard HUIT service management channels
2. Consult with business owner and customer technical contact on:
    a. Eligibility for HarvardKey integration
    b. Appropriate authentication and authorization design
3. Configure the Identity Provider (IdP) based on the registration request submitted by the customer and any subsequent update request
    a. Apply authorization filters to ensure that users have least privilege
    b. Set Harvardkey idle session timeout to two hours
4. Notify application owners with problems or faults with a registration
5. Maintain knowledge articles and resources

Consequences of Policy Violation

1. IAM will monitor for compliance with the policy. IAM will work with application owners to develop a remediation plan if an application is found to be in violation of the policy. If the remediation plan is not implemented within a reasonable timeframe, IAM, in consultation with the School Security Officer, may disable registrations that are determined to be in violation of the Application Integration Policy. Registrations that are disabled may regain access once made compliant.
2. Individuals knowingly providing inaccurate information in their annual attestation or violating the Application Integration Policy may be subject to disciplinary action.

Related Resources / Reference Links

- HarvardKey Application Integration Services
- HarvardKey Affiliation and Assurance Tier Classifications
- Harvard Information Security Policy
- Accessible Technology Procurement and Development Policy
- Data Privacy Guiding Principles
- Directory Listing Policy
- FERPA Overview
- General Records Schedule
- Internet2 Wiki - Signing & Encryption Keys
- School Security Officers
- Strategic Procurement Office

Contact/Responsible Offices

This Policy has been developed with input and contributions from the following offices and schools:

- Academic Technology, HUIT
- Administrative Technology Services, HUIT
- Information Security, HUIT
- Library Technology Services, HUIT
- Technology Partner Services, HUIT
- Harvard Law School
- Harvard Medical School
- Strategic Procurement Office

These offices will be engaged in regular review of and revisions to this Policy.

Identity and Access Management Services (IAM), Harvard University Information Technology is responsible for maintaining this Policy and acting as a resource for schools and units with questions regarding this Policy. It will also provide centralized training resources regarding this Policy.

Information Security offices in the schools and the University Chief Information Security and Privacy Officer will be responsible for granting exceptions to the policy.

Review Period

The Application Integration Policy will be reviewed and updated – as needed – on an annual basis but no less frequently than every three years.

Revision History

Version 1.0 - Initial Version
Version 1.1 (Added requirement to maintain data and contacts and to specify at least 1 Registration Manager per application) 2022-12-09

Glossary

Application is a computer program designed to help users perform an activity or task.

Application Owners are users responsible for deciding the business needs of applications with respect to IAM. They work with the IAM program team on how best to integrate their applications with IAM services, as well as directing the configuration of their applications. In the HarvardKey Application Registry (HKAR), these individuals will be assigned the Registration Manager contact type for any applications they own.

Application Integration is the process of enabling independently designed applications to work together.

Assertion or "SAML assertion" is a set of XML-based statements returned from an Identity Provider, e.g. HarvardKey IdP, to a Service Provider(SP) to make access-control decisions. Three types of statements are provided by the SAML protocol:

- Authentication statements
- Attribute statements
- Authorization decision statements

Attributes are units of personal information about end users of an application (e.g. name, unique identifier, primary affiliation) that may be released to the application for the purposes of authorization, account provisioning, and facilitation of the end user's session.

Authentication or "logging in", is the process of validating that people or entities are who they say they are.

Authorization is the process of determining if a user has the right to access a service or perform an action.

Authorization Filter is a general purpose filter created from one or more read-only IAM reference group(s) in Grouper that can be applied to a HarvardKey registration to provide a foundational level of authorization as part of the authentication process.

Attestation is the process of reviewing your application registration data.

Bundle Groups are comprised of multiple reference groups from various affiliations (e.g. student and employee reference groups) bundled together in one group (e.g. All Student and Employees).

Dry Run is where the HarvardKey team builds a parallel production environment with the upgraded code and directs traffic to the parallel environment for a limited period of time during a low-volume period. This allows application teams to test authentication for their systems in the production environment to confirm that there are no issues prior to the formal release. If any issues are identified the HarvardKey team can work to resolve them during or after the dry run window. After the dry run

window traffic is directed back to the primary production environment. If significant issues are found during the dry run the window can be cut short to avoid user impact.

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

HarvardKey is a unified login credential for users across the Harvard Community, supported by the service that authenticates users of online applications created by or affiliated with Harvard. Authenticating with HarvardKey verifies users' identities in order to allow them to access applications; to do this, the user provides a unique login name (in the form of an email address) and confirms that identity by submitting the correct password. Two-step verification (see below) is available with HarvardKey for an extra level of security assurance.

Identity Provider (IdP) is a system that validates the identity of a user in a federated system. The service provider (or SP; see below) uses the IdP to get the identity of the current user.

MemberOf Attribute Groups that a user is a member of.

Reference Groups are institutionally meaningful, programmatically generated read-only groups based on authoritative sources, such as the IAM identity registry organized by role and affiliation (e.g. all students in a school).

Service Provider (SP) is a system that provides a generic service to the user in a federated system. To users, a service provider is the same thing as the application they are trying to use.

Technical Contact is the developer(s) familiar with the details of the technical implementation. They are the point of contact in the event of a technical incident.