Updated 7/28/2020

HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

HarvardKey Authentication Service Registration Form

Before You Begin

Please read through this opening information before you complete the registration form. Gaining an understanding of the concepts outlined here will help with the integration of your application into HarvardKey services.

HarvardKey services include:
Authentication – confirming a person has working credentials to log into Harvard applications,
Authorization – confirming the credentials presented have an active affiliation that allows them access to your application, and
Attribute Release - passing specific data about the user over to be consumed by the application.

Every application will use both authentication and authorization. Attribute release is optional (but recommended). An important concept for any application owner to recognize is that authentication credentials do not expire when affiliation with Harvard ends. Meaning, when someone leaves the University their HarvardKey will continue to function. Which means, to protect your online resource, an application must both authenticate and authorize users. Authorization will stop anyone without an active affiliation (based on group membership) logging into your application. In rare instances, authorization can be waived (with a valid reason) but we will work with you to put a basic authorization filter (using groups) in place.

Before submitting this form, please make sure your procurement processes have been completed and a signed contract is in place. Check out Section V of the Strategic Procurement Manual for more details. The Strategic Procurement Contracts team can provide further assistance and training as needed.

Harvard IAM is part of the InCommon Federation (we are an InCommon IdP) so that we can support users from other member institutions if you require them to be able to log into your application. Much more information is available on our website: https://iam.harvard.edu/resources/incommon

Attributes to be released are reviewed and approved for every application. We strongly recommend using the eduPersonPrincipalName attribute (EPPN) -- because it is unique and doesn't include personally identifiable information about people -- whenever possible. Harvard requests that you use Preferred Name attributes (not Official Name) to support our commitment to Diversity & Inclusion. We also will confirm how the attributes will be stored and used in your application. Privacy compliance must be ensured for Harvard user information.

If you are working with a vendor, have them identify a technical representative who can provide the required information (SP metadata, entity IDs, endpoint URLs, etc.) needed in this form. Having meetings that include a knowledgeable vendor technical rep can really help facilitate the integration process.

Along with this form, you will need to fill out an 'Attributes Being Requested' spreadsheet (for any attributes you would like released to your application). If you are using the SAML Authentication protocol, also generate and attach metadata when you send in your form please.

Questions about this information or the form?

Email iam_help@harvard.edu with the subject "Request to Integrate with HarvardKey."

Updated 7/28/2020

Please submit this form to register your application for HarvardKey authentication, authorization and optional attribute release services. You can type directly into this document and use as much space as you need for your answers. Do not worry if that changes the pagination of the document.

App Owner Contact Details

Please provide at least one contact name for each role below. A single person may fulfill more than one role; however, there should be at least two different names listed in conjunction with an application.

Departmental Email: A departmental email address that will not change with staff turnover (ex: iam@harvard.edu)
Email:

Requestor: Harvard employee requesting the registration of this application
Name: Email:
Name: Email:

Technical Contact: Developers(s) that know the details of the technical implementation. The Technical Point people for the integration with IAM services and will be the future point of contact in the event of a technical incident.
Name: Email:
Name: Email:

Technical Practice Owner: Responsible for the overall design and implementation of your application.
Name: Email:
Name: Email:

Business Owner: Responsible for sponsoring the implementation and defining scope and approach.
Name: Email:
Name: Email:

Project Coordinator: Leads work with the vendor and/or coordinates the team.
Name: Email:
Name: Email:

About Your Application:

The information you provide on this form will be kept as part of the permanent record for this application integration with HUIT IAM Services, so please take time to answer all the questions on the form clearly and completely. Thank you in advance!

Name of application:

Please describe the purpose of this application:

In general terms, please describe the type of users who will access the application:

Will your application also support any local application credentials in parallel to Harvard Key? If yes, please describe how they will be used (e.g., emergency “backdoor” access, etc.)

User Authorization:

Please describe the population who should have access to your application? (for example: any active Harvard user, alumni, students in a specific school)

Based on the answer we’ll help figure out the basic reference groups to use for authorization. All applications will receive (at the least) our standard application authorization group (All Current HUID Holders).

Additional authorization options are available (but need to be discussed). Please check any you would prefer to use:

- ☐ Using an application-specific group as an authorization filter
- ☐ Using a list of named users within the application (local permission list)
- ☐ Using an LDAP or API-based query to integrate an authorization decision
- ☐ Other (please specify)

Is this an in-house-developed application? If yes, where/how is it hosted?

Is this a SaaS implementation (solution hosted by the vendor)? If yes, who is the vendor?

Provide a link to any vendor documentation regarding integration with Single Sign On (SSO):

If working with a vendor, does a contract exist at this time? ◯ Y / N ◯

Whose name (Harvard employee) appears on the contract?

Did your department work with Harvard Strategic Procurement? ◯ Y / ◯ N /Not Sure ◯

Name of SP Contact:

Has this contract been reviewed by Harvard OGC? ◯ Y / ◯ N / Not Sure ◯
Name of OGC Contact:

Authentication Details: Identifiers

Do you expect external users (those with no HarvardKey but a credential from their home institution) to authenticate via federatedlogin (e.g., InCommon)? ◯ Yes / No ◯

HUIT strongly recommends accepting an opaque unique identifier (EPPN) to protect users' privacy. This type of identifier consists of a sequence of letters and numbers. It does not include a name or other personally identifiable information. Other identifiers can be requested for inclusion in the authentication response if there is a business need for the data.

Many vendor applications expect email to be an unchanging unique identifier. In the case of HarvardKey, Login Name is released as the 'mail' attribute. Please be aware that Login Names are subject to change over time; for example, when individuals move between schools.

Requested Attributes/Privacy Details

Please use the 'Attributes Being Requested' spreadsheet to review the list of available attributes and submit a completed copy of the spreadsheet as part of your request. You will need to fill out Column F and G for any attributes that you are requesting. All requests for attributes are subject to review and approval.

Will your application use the attributes it receives to create a browsable directory of users? ◯ Yes / No ◯

Will normal (non-administrative) users of your application have the ability to view data about other users of the application?

Will application administrators be able to view the user attribute data of other users?

Will attributes be stored in a database related to your application? If yes, how will that database be used? (e.g. reporting, authorization of users to the service, etc.)

Session Lifetime

HUIT can configure your implementation to force authentication at every login (and not use SSO). In this configuration, users will be prompted to provide their login name and password, even if they have recently provided these credentials to another application within the authentication system. This type of non-SSO configuration is appropriate for applications managing sensitive data (e.g. financial, personally identifiable).

Do you want to disallow automatic single sign-on? ◯ Yes/No ◯

If you are using the single sign-on function, how long should the user session persist?

Note: if you request more than 2 hours, we will need to request special approval from IT Security. Also, if your application has a way to configure the session lifetime you should consider your user's experience and make sure it matches the session allowed by HarvardKey. The two work independently and if they differ it can cause confusion

This final section has to do with information needed to set up your app with the authentication protocol that you plan to use – fill out the section for either SAML or CAS. A Service Provider (SP) initiated SSO is preferred but we can also support IdP initiated SSO if that is required.

For SAML/SP/Shibboleth: Entity ID

Please generate and attach your SP metadata file when you send this form.

Please provide the application's entity ID(s) in URL form:

For example: https://huit.harvard.edu/identityaccessmgmt/ourCoolApp/sp

Provide your Assertion Consumer Service (ACS) URLs (for each environment that you will be integrating):

Prod:

Prod -1:

Prod -2:

Prod –3:

Can you accept an encrypted assertion response? ◯ Yes/No ◯

(we prefer encrypted, but can support an unencrypted assertion if that is required by the SP)

Do you need to use Name ID? What is the expectation for its use?

The ACS is the URL to which the IdP should send the SAML/Shibboleth authentication response. If you are not intending to use SAML/Shibboleth POST binding, please indicate that here:

For CAS or CAS-with-Attribute Release: Endpoint URL

Please list the endpoint URL(s) (for each environment that you will be integrating):

Do not include any path or context, wildcard, "/" or "/*" at the end of the URL.

To protect a specific path or context on your server or instance, configure the CAS client on your

server. Some examples of paths you can configure on your side are https://myapp.harvard.edu/pages or https://myapp.harvard.edu/secure/*

All endpoint URL(s) are registered against the University's production environment (Prod) by default. Customers' production, test, stage, and/or development instances will all "run in Prod." If there is a business requirement, customers may register by special request for the HUIT stage environment, which is generally used for testing changes to the authentication systems themselves.

Acknowledgment & Signature:

By signing below (or by submitting this form from your Harvard email address) you certify that you have read the following important information and understand the impact for all your application instances that will be registered with HarvardKey services.

- I certify that I fully understand that the only pages to which users may be redirected for entering their authentication credentials (e.g., ID and password pair) are the official University login pages
- I acknowledge that the user must be redirected to these pages and the pages must not be presented to the user via web frames or any other method
- I acknowledge that under no other circumstances may a web page be deployed that requests the user to enter Harvard University authentication credentials
- I understand HarvardKey credentials never expire, and users will still have working ID and set of credentials after they end Harvard affiliation
- I agree that as a recipient of attributes other than EPPN, I understand that data provided in the assertion must not be distributed beyond the local system, and must only be used for the purpose requested in this application
- I certify that the answers I have provided in this form are accurate, to the best of my ability.

Signature:

_____

If you are submitting this form from a harvard.edu email account it does not require a signature.

Please submit this form, the attribute spreadsheet and your SAML metadata (if applicable) to iam_help@harvard.edu