Authentication & Attribute Registration
CAS/SAML/SP Usage Request

Important: *In most cases, use of authentication as the sole method of authorizing access is inadequate. Notably, individuals who are no longer affiliated with Harvard, but remember their credentials, can still authenticate. Therefore, you are strongly advised to provide a method of authorization in addition to authentication.*

Questions about this form? Email iam_help@harvard.edu with the subject "Authentication Service Registration Form."

App Owner Contact Details

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

Requestor: Harvard employee requesting registration of this application.

Name: Harvard email:

Name: Harvard email:

Technical Contact: The main developer and others knowledgeable about the technical implementation. These are the point people for integrating your application with IAM services, and points of contact in the event of a technical incident.

Name: Email:

Name: Email:

Technical Practice Owner: The person responsible for the overall architecture and implementation of your application.

Name: Harvard email:

Name: Harvard email:

Business Owner: The person who commissioned the application and is responsible for defining its scope; he/she works with app technical team and IAM in formulating what information is sent from IAM services to the application.

Name: Harvard email:

Name: Harvard email:

Project Coordinator: For vended applications, the project manager acting as vendor liaison.

Name: Email:

Name: Email:

Group Email: A departmental email address that will not change with turnover of personnel.

Email:

About Your Application

Please describe the purpose of your application:

Please describe the user populations your app will serve and the login credentials they might use (e.g. HKS alumni, hospital employees, Harvard faculty, etc.) *This helps determine what login types appear on the login screen.*

(continued on page 2)

Who is hosting your application, and who is administering it (e.g. granting access rights)? *Examples: Administered by Harvard personnel and hosted at Harvard (e.g. PeopleSoft); third-party administered and hosted (e.g. ASPIRE); Harvard-administered but third-party hosted (e.g. HUIT's Service Now instance)*

If you are working with a vendor, has your contract been reviewed by OGC? ☐ Yes ☐ No
If yes, whose name (Harvard employee) appears on the contract?

Please describe how you will verify that the user is eligible to access your application (i.e. using attributes from the SAML/ Shibboleth assertion, from University LDAP, or from the data warehouse), along with authorization rules within the application:

Do you expect external users (i.e. from other universities — this does not include HMS affiliates or Harvard Alumni) authenticating via federated login/InCommon?

☐ Yes ☐ No

Will you request any attributes other than EPPN (see "Requested Attributes" section below for more details)?

☐ Yes ☐ No

If you checked "Yes" to either of the preceding two questions, skip to the "Requested Attributes" section below. Otherwise, please complete the "Authentication Only" section below and skip the "Requested Attributes" section.

Authentication Only

We strongly recommend accepting only an opaque unique identifier (EPPN) for the user — which consists of a sequence of letters and numbers, and doesn't include a name or other user information — unless your app relies on an identifier such as HarvardKey, eCommons ID, eXtended ID, or Advance ID for mapping and subsequent authorization.

If your application cannot accept an EPPN in the response, please explain why.

What login types does your app expect/need? If more than one, indicate default.

☐ HarvardKey

☐ Harvard Medical Community Intranet ID (eCommons ID)

☐ Advance ID (identifier used by the alumni repository)

☐ eXtended IDentification number (XID; an identifier available for people without a current Harvard University affiliation and therefore not eligible for a HUID)

Default:

Please note: Assertion will contain EPPN or login ID, pending review of your justification.

(continued on page 3)

Requested Attributes

IAM holds a number of attributes about each user, but we encourage applications to use the standard set of attributes recommended by InCommon (listed below). Please select what attributes you need from the list, or specify any attributes not listed. If you don't strictly need a personally identifiable attribute, such as a user's surname, consider not requesting it. All attribute requests except EPPN go through an approval process.

- ☐ *eduPersonPrincipalName* (EPPN): Unique opaque identifier that will never be reassigned to another user
  We strongly recommend accepting only EPPN — which doesn't include a name or other user information — unless your app relies on HUID for mapping and authorization. If you cannot use EPPN, explain why below.
  - ☐ Harvard University Identification Number (HUID)
    Only for applications that cannot accept EPPN; please explain below
- ☐ *eduPersonScopedAffiliation*: One or more of faculty, staff, student, affiliate, or member
- ☐ Additional attributes (please specify):
- ☐ *sn*: Single-string value containing user's family name or surname
- ☐ *givenName*: Single-string value containing the part of the user's name that is not their surname or middle name
- ☐ *mail*: Email address of record in Harvard University Identity Database
- ☐ *displayName*: Single-string value indicating preferred name for display purposes (i.e. a greeting or directory listing)

Please describe the business need for the attributes requested. If appropriate, describe as well the reason for your application's inability to accept an opaque unique identifier and your resulting request for HUID instead.

Will your application be using the attributes it receives (i.e. address, email, etc.) to create a directory or similar product/service?

☐ Yes ☐ No

Who will have access to the attribute data? Select all that apply.

☐ The application user, viewing data about him/herself
☐ Other application users, viewing data about each other
☐ Application administrators

Will attributes be stored in a database? ☐ Yes ☐ No

If so, please describe how, specifically explaining security measures:

(continued on page 4)

Session Lifetime

Please define a session lifetime between 5 minutes and 12 hours:

The authentication system uses your application's registered session lifetime to determine whether the user must authenticate by manually entering a name/password, or if the user is considered already authenticated because of a past explicit "login" and "single sign-on" (SSO) features of the authentication system. You can configure your implementation to request forced authentication, in which the users will be prompted to provide name and password, even if they have recently provided these credentials to the authentication system.

Your software may also let you configure a session lifetime. It is best to consider the user experience in light of both of these session lifetimes, since they are independent of each other.

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

Please list your endpoint URL(s):

Example endpoint URLs: https://myapp.harvard.edu *or* https://myapp-test.harvard.edu *or* https://example.xyz.com*. 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.

For SAML/SP/Shibboleth: Entity ID

Provide your app's entity ID(s) (example: https://huit.harvard.edu/cadm_huit_identityaccessmgmt/ourCoolRegistrationApp/sp):

Additional Technical Details

Please attach your SP metadata file when you send this form. Additionally, provide your Assertion Consumer Service (ACS) URLs ...

Production Instance ACS:

Test Instance ACS:

Development Instance ACS:

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 email ithelp@harvard.edu with the subject "SAML application needs non-standard binding." Please note that the Harvard IdP only accepts SAML2 authentication requests.

Acknowledgment & Signature

☐ 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; furthermore, 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.

Under no other circumstances may a web page be deployed that requests the user to enter Harvard authentication credentials. I understand these credentials never expire, and users will still have working ID and set of credentials after they end Harvard affiliation.

☐ 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.

Signature of Harvard requestor (must be employee) Date

Submitting this form from a harvard.edu email account does not require a signature.

Submit this form and its supporting documents to **iam_help@harvard.edu**
with subject "Authentication Service Registration Form"