## Purpose of Questionnaire

A questionnaire that would allow on boarding Service Providers to 'self-assess'; using a line of questioning that presents guidance, recommendations, and criteria depending on the answers given.

Link to the Questionnaire:
https://docs.google.com/forms/d/e/1FAIpQLSfaDZ0B_qnOqRAsiP1oNVKI1aYsErmCQjXRWecztIgOYJQwVw/viewform

## I. Onboarding Questionnaire - Opportunities to Fill Out and/or Review

A. When should a Service Provider fill out the questionnaire?
   a. During a home institution's Request for Proposal process; as part of a vendor evaluation and before any purchases are made.
   b. A requirement as part of joining InCommon
   c. An optional step for non InCommon members to follow to determine if they are technically capable to join InCommon and become a functioning member.
   d. At point of becoming a site admin via the InCommon Administration tool
   e. As part of an annual cycle/review period; to ensure responses are kept accurate

## II. Onboarding Questionnaire - Question Outline

**A. Establishing Trust**
   a. Is your organization a member of the InCommon Federation?
   b. Has your organization registered your service's metadata with the InCommon federation?
   c. Has your organization defined a process for keeping your metadata up to date?
   d. Does your application consume, refresh, and verify the signature on InCommon metadata routinely?

**B. Technical Interoperability**
   a. Does your application implement SAML2 using the recommended software?
   b. Have you generated your SAML (X.509) certificate using the InCommon security and trust requirements?
   c. Will your application be authenticating users via more than one Identity Provider, either within a single institution or within a Federation?

**C. Identifiers and Attributes**
   a. Does your application support a relevant portion of the InCommon Attribute Set?

b. Is your application able to support user identification using at least one of the eduPerson or SAML V2.0 Subject identifiers?
c. Please specify those minimum attributes that your application requires from its user community?

**D. Authorization**

a. Will your application be using authorization to allow or restrict access?
b. How will your application be authorizing its user population?

**E. User Experience**

1. <Checklist>

## III. Onboarding Questionnaire - Criteria being vetted

### A. Establishing Trust

DO register your Service Provider's metadata with the InCommon federation
DO define a process for keeping your Service Provider's metadata up to date
DO configure your Service Provider to verify the signature on metadata
DO consume and refresh the InCommon metadata at least daily

### B. Technical Interoperability

DO follow the InCommon security and trust requirements for your SAML certificate(s)
DO implement SAML2 using the InCommon recommended software
DO use a SAML implementation which conforms to the Kantara SAML v2.0 Implementation Profile for Federation Interoperability

### C. Identifiers and Attributes

DO support the InCommon Attribute Set
DO support a varied set of userid identifiers
DO commit to a stable user identifier *(i.e will not be reassigned and has minimal risk of changing)* that is only assigned to a single individual *(i.e. has the necessary scope to ensure uniqueness and is not shared across multiple individuals)*
DO support the InCommon recommendations for user identifier standards *(i.e. the eduPerson and the SAML V2.0 Subject Identifier Attributes Profile Version standards)*
DON'T mistake eduPersonPrincipalName for a valid email address
DON'T assume email address can be treated as a unique user identifier (and cannot be released as a unique identifier) without prearrangement with the Identity Provider.

### D. Authorization

DON'T assume successful authentication means the user is authorized for the service.

DO decide on a consistent approach for authorizing user access to your application *(i.e the eduPerson standard and in particular the eduPersonEntitlement or eduPersonScopedAffiliation attributes)*
DO be clear about where the allow/deny decision logic is evaluated.

### E. User Experience

DO provide a consistent user experience for how user information *(i.e. attributes)* are presented and shared within the application

**[1]** **https://kantarainitiative.github.io/SAMLprofiles/fedinterop.html**