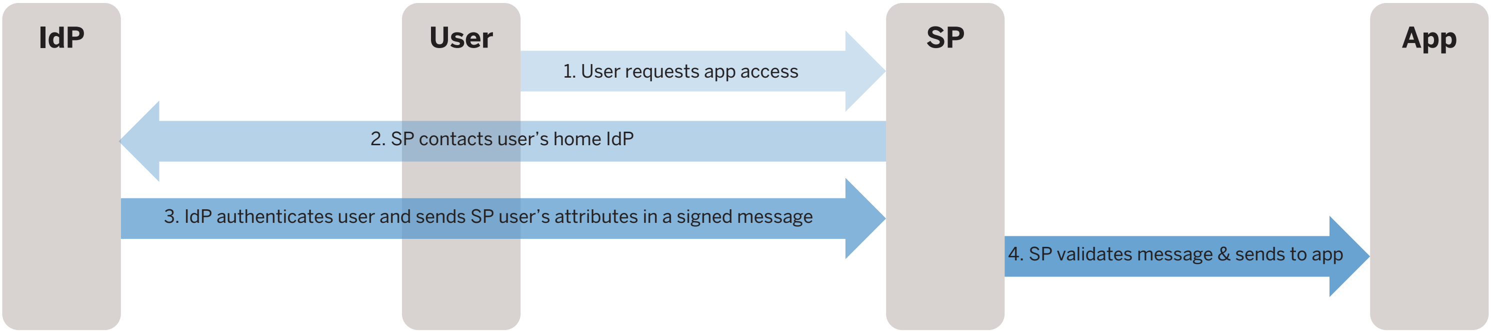
Federated Identity at Harvard
The InCommon Approach

HARVARD UNIVERSITY
Information Technology
IDENTITY & ACCESS MANAGEMENT

How Does Federated Identity Work?


IdP
User
SP
App
1. User requests app access
2. SP contacts user's home IdP
3. IdP authenticates user and sends SP user's attributes in a signed message
4. SP validates message & sends to app

1. When a user requests access to an application at a different institution, the service provider (SP) in front of that application receives that request
2. The SP contacts the user's "home" identity provider (IdP)
3. That IdP authenticates the user, looks up his or her attributes, and then sends those attributes in a signed message to the application SP
4. The application SP validates the message, and may transform the attributes for ease of use by the application (such as relabeling a value for *email* to *mail*)
5. The application uses the attributes to confirm whether the user is authorized for access

Why Use InCommon Federation?

- Federation organizations such as InCommon allow SPs to avoid issuing secondary credentials to individuals because they trust a user's home institution to validate identity
- The exchange of information, as appropriate, about federation users and resources can make it easier to enable collaboration
- All InCommon participants agree on the same policies and procedures related to identity management and the passing of attributes
- Instead of one-to-one relationships, federation allows one-to-many relationships
- Federation does require negotiating attribute release for individual applications; however, the technical implementation is streamlined and does not require extensive customization

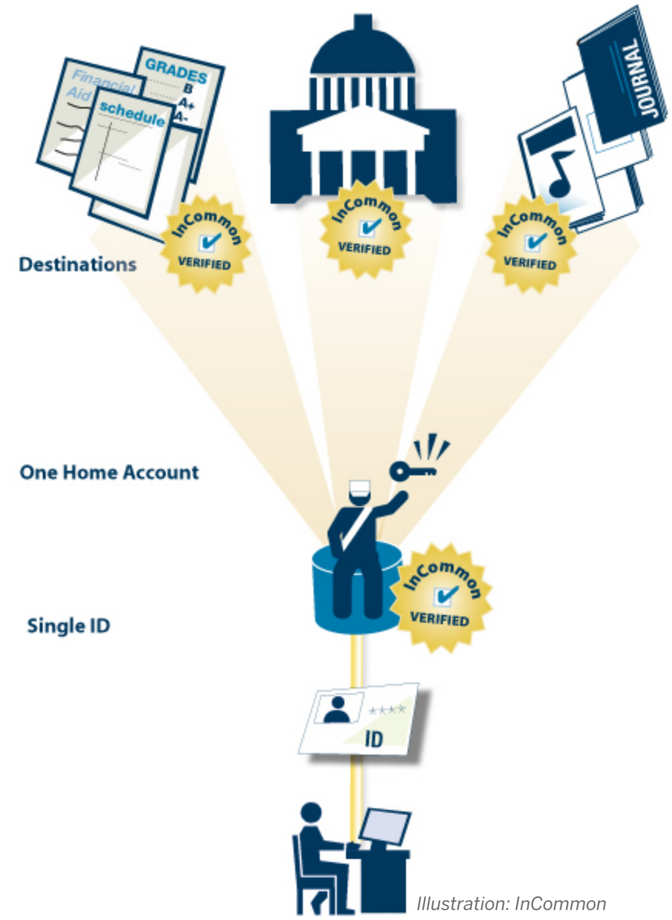


Illustration: InCommon

Federation Benefits

- Single sign-on is much more convenient for users
- Services no longer manage user passwords
- Reduced service desk load
- Standards-based technology
- Privacy is under the control of the home organization and the users themselves

Learn more about federation and Harvard's Identity & Access Management program at iam.harvard.edu