HARVARD UNIVERSITY
Information Technology

InCommon Overview

for Harvard-Affiliated Hospitals

Agenda

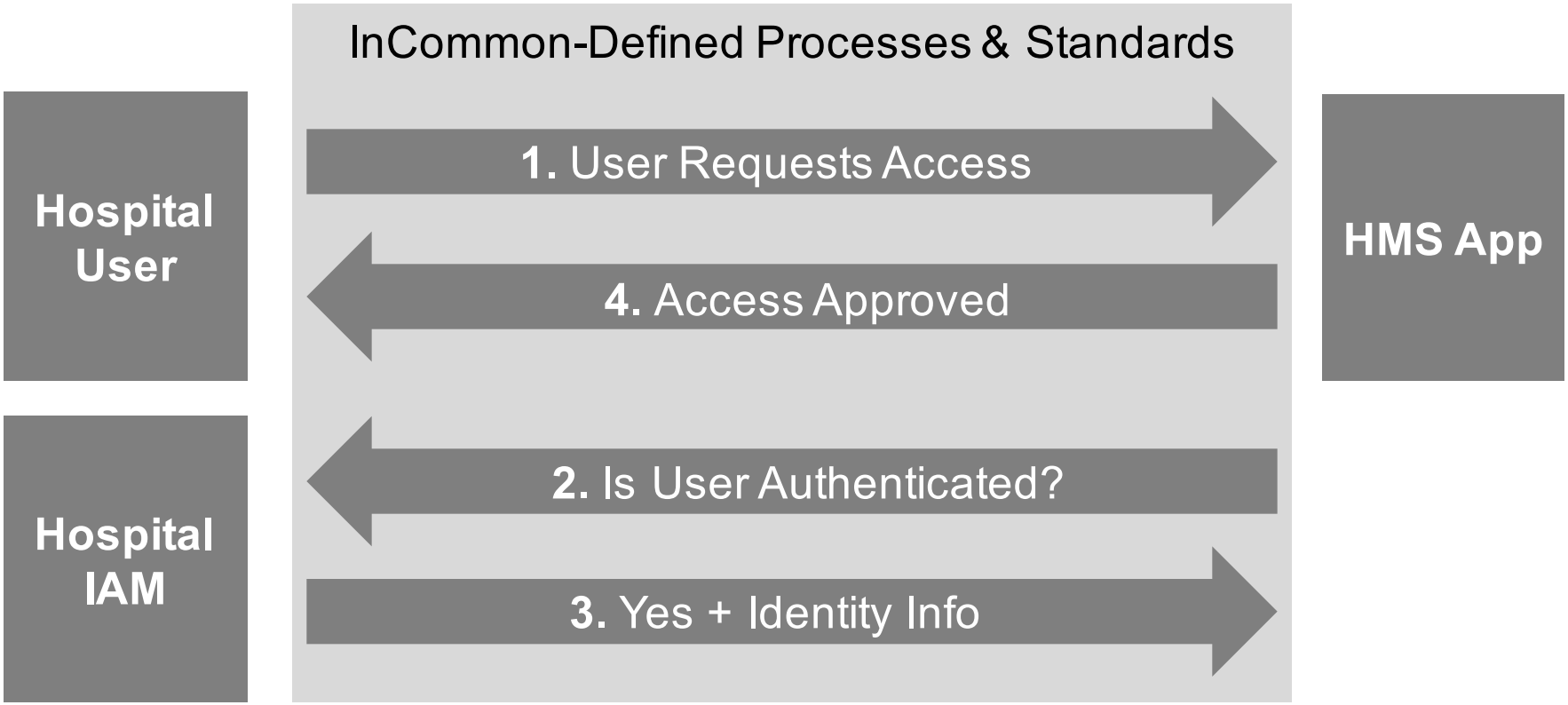
- What is the InCommon Federation?
- How Does InCommon Federated Identity Work?
- Why Use InCommon Federation?
- “If We Join InCommon, Who Can Access My Data?”

What is the InCommon Federation?

The InCommon Federation provides an open-standards-based, SAML-compliant common framework for trusted, distributed access management of online resources.

- Operated by Internet2
- Identity management federation serving 8 million end users *(IPEDS data, October 2014)*
- The first trust framework approved for LOA Level 1 and 2 access to federal resources by the Federal Identity, Credential, and Access Management (FICAM) program
- Used by NIH and NSF to provide secure access for external users without the need to create new accounts
- Harvard's InCommon implementation is a FICAM Trust Framework Solution (TFS) approved identity service — learn more at http://www.idmanagement.gov/approved-identity-services

How It Works: Overview

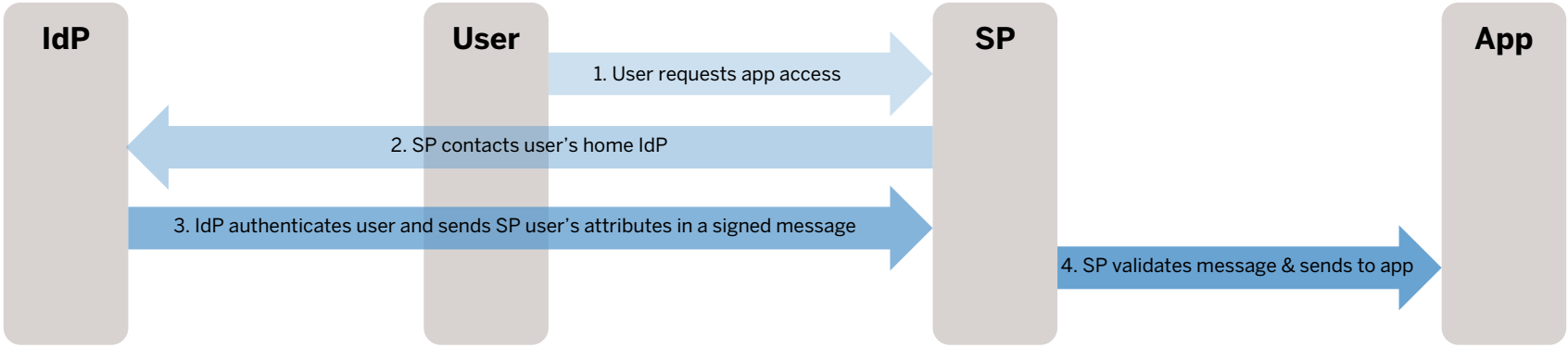


How It Works: The Technology

There are two critical components behind how federated identity works:

- **Identity Provider (IdP):** As a gateway for providing identity access through InCommon, Harvard's IdP validates that a user is authenticated by Harvard when accessing InCommon-managed services. Hospitals would do the same in an InCommon-based solution — each Hospital would use a similar IdP to validate authentication and provide identity information for HMS applications.
- **Service Provider (SP):** An SP intercepts requests made to applications, stepping in to manage validation and requests for identity information. Since this function is specific to managing application access, it would not be required for Hospitals unless they wish to trust Harvard's IdP for accessing Hospital applications.

How It Works: Putting It All Together



1. When a user requests access to an application at a different institution, the SP in front of that app receives the request
2. The SP contacts the user's "home" IdP
3. That IdP authenticates the user, looks up his/her attributes, and sends those attributes in a signed message to the application SP
4. The SP validates the message, may transform attributes for ease of use by the app (i.e. relabeling *email* to *mail*), and sends the app the attributes
5. The app gets the attributes via standard web programming methods, and then uses them to confirm whether the user is authorized

Why Use InCommon Federation?

Today	Imagine …
Because the HMS system is dependent upon communication from each Hospital, deprovisioning happens rarely — if at all	Deprovisioning is automatic — when the Hospital updates its system, access to Harvard applications is automatically updated too
Users forget IDs and passwords because they may not use Harvard applications often enough to keep them in memory	A user's regular Hospital credential allows them access to their Harvard applications
A new Hospital user's access can be delayed because of HMS communication and prioritization	When a user is provisioned into a Hospital system, they're also granted access to their Harvard applications
The HMS solution is proprietary, with support dependent upon HMS	The codebase is standard, implemented once, and supported by an established network of existing organizations

“If We Join InCommon, Who Can Access My Data?”

InCommon federation *enables* access, but doesn’t *force* access.

For the Hospital IdP, this means:

- Hospitals choose which InCommon SPs to interact with
- They also choose which attributes to release to a given SP about a given user

For the Harvard SP, this means:

- Resource owners choose which InCommon IdPs to interact with
- They also maintain control of which users from those IdPs get access, and under what rules

Questions?

Thank you!

HARVARD UNIVERSITY
Information Technology