



**2015**  
**TECHNOLOGY**  
**exchange**

**OCTOBER 4-7**  
**CLEVELAND OH**

**FEDERATION INTEROP AND EDUGAIN BRIEFING**

**Walter Hoehn, U. Memphis / Nick Roy and Tom Scavo, InCommon**

# Federation Interop: What's Up With That?

## Agenda

- Why a Federation Interop Working Group?
- Scope of Work
- Current Status
- What's Next?

# Why a Federation Interop Working Group?

- Aren't there already at least a couple of those?
  - Yes
  - This is focused first on the groundwork needed to support multilateral, full mesh SAML federations in use in the research and education sector
  - Chartered by the TAC to help drive solutions to concrete problems in InCommon
- Want to be able to hand the first work product to SAML software implementers who want to target our federation model
- Many such participants in the working group (thanks!)
- Their support is fundamental to continuing to deliver value to InCommon participants

# Scope of Work

- Provide creators of SAML products with a concrete set of requirements for interoperating within InCommon
- Outline SP and IdP operational and deployment practices that are necessary for interoperability with minimal or no administrator involvement
- Provide direction concerning the most common interoperability problems encountered by InCommon participants.
  
- Recognition of wider applicability
  
- Stack
  - Implementation Profile
  - SAML2Int
  - Document(s) covering higher-ed-specific or InCommon-specific practices



OCTOBER 4-7 · CLEVELAND OH

# Current Status

- Call for Participation - July 7, 2015
- Began Weekly Conference Calls - August 10, 2015
- Face to Face meeting during Advance Camp - October 5, 2015
  
- Matrix - common interoperability problems
  - Categorized (Software vs. Operational)
  
- Began work on Implementation Profile Specification
  - “SAML V2.0 Federation Implementation Interoperability Profile”
  - Building on pre-existing materials
  - Coming Soon: workable draft that can be reviewed by a wider audience



OCTOBER 4-7 · CLEVELAND OH

# What's Next?

- Complete Draft of Implementation Profile - Submit to TAC
- Solicit feedback within InCommon
- Engage other communities - REFEDS/Kantara Initiative
- Publish profile
- Federation lab (GÉANT and Kantara) Test Suite
- Proposed updates to SAML2int



OCTOBER 4-7 CLEVELAND OH

# Global Interfederation

## Federation at Scale



OCTOBER 4-7 CLEVELAND OH

# Contents

1. What is eduGAIN?
2. eduGAIN Checklists
  - a. eduGAIN for Organizations
  - b. eduGAIN for IdP Operators
  - c. eduGAIN for SP Owners



OCTOBER 4-7 CLEVELAND OH



# What is eduGAIN?



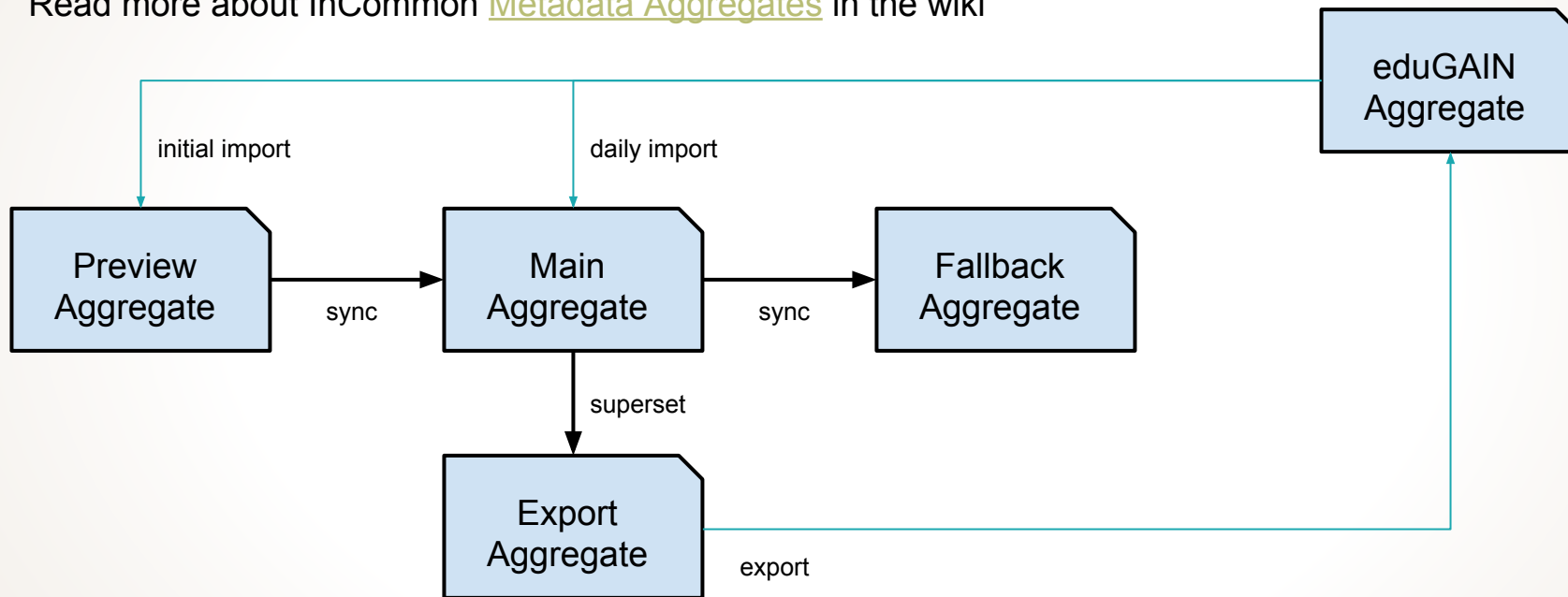
- eduGAIN = EDUcation Global Authentication INfrastructure
- eduGAIN is a *metadata aggregation service* run by GÉANT for the higher ed community worldwide
- The eduGAIN service routinely imports metadata from dozens of participating federations, aggregates that metadata into a single signed document, and then serves the aggregate file from a well-known HTTP location
- eduGAIN operates at the federation level, that is, the eduGAIN aggregate is not intended to be downloaded directly by IdP operators and SP owners
- InCommon signed the eduGAIN Declaration in April 2014



OCTOBER 4-7 · CLEVELAND OH

# InCommon Metadata Pipeline

Read more about InCommon [Metadata Aggregates](#) in the wiki



# Importing eduGAIN Metadata

(as of 2015-09-27)	<b>BEFORE</b>	<b>AFTER</b>
<i>Metadata file size:</i>	16062158 bytes	32322949 bytes
<i>Number of registrars:</i>	1	35
<i>Number of organizations:</i>	573	2106
<i>Number of SAML entities:</i>	2960	5269
<i>Number of IdP roles:</i>	412	1836
<i>Number of SAML2 IdP roles:</i>	406	1828
<i>Number of SP roles:</i>	2548	3435
<i>Number of SAML2 SP roles:</i>	2501	3354



OCTOBER 4-7 · CLEVELAND OH

# Metadata Registrars

The five largest metadata registrars (as of 2015-09-30):

Registrar ID	# of entities	# of IdPs	# of SPs
<a href="https://incommon.org">https://incommon.org</a>	2962	412	2550
<a href="http://ukfederation.org.uk">http://ukfederation.org.uk</a>	1216	513	704
<a href="https://federation.renater.fr/">https://federation.renater.fr/</a>	257	238	19
<a href="http://cafe.rnp.br">http://cafe.rnp.br</a>	114	114	0
<a href="http://www.idem.garr.it/">http://www.idem.garr.it/</a>	98	69	28

For a complete list of metadata registrars in higher ed:

<https://incommon.org/federation/info/all-entities-mdq-beta.html>



OCTOBER 4-7 · CLEVELAND OH

# Prepare for Metadata Import

The Shibboleth IdP is known to be sensitive to large metadata aggregates. To prepare for the import of eduGAIN metadata, InCommon recommends:

1. Allocate **at least 1024MB of heap space** in the JVM
2. Enable DEBUG-level logging on the following Java classes:  
V2: org.opensaml.saml2.metadata.provider.AbstractReloadingMetadataProvider  
V3: org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver

Read more about how to [protect against failed metadata processes](#)



OCTOBER 4-7 CLEVELAND OH

# The Export Aggregate

A small group of InCommon participants have been exporting their metadata to eduGAIN in pilot mode since the summer of 2014:

- [University of Wisconsin-Milwaukee](#)
- [LIGO Scientific Collaboration](#)
- [Internet2](#)
- [National Institutes of Health](#)

Currently 16 R&S SPs are included in the [InCommon Export Aggregate](#). Full eduGAIN participation is scheduled to begin early in 2016.



OCTOBER 4-7 CLEVELAND OH

# User Interface: Metadata Export for SPs

SP owners choose to **opt-in** to metadata export:

## Metadata Export

If you want your SP metadata to be included in the InCommon export aggregate, check the box below. If you do **not** want your SP metadata to be exported, leave the box unchecked.

**IMPORTANT.** If you do **not** export your SP metadata, and your SP has a dynamic discovery interface, then you should filter global metadata at the SP, otherwise some users may have a failed login experience. Configure your SP [using the Registered By InCommon Category](#) if necessary.

*Include this SP metadata in the InCommon export aggregate*

Questions? Visit our wiki for a complete metadata export FAQ: [URL]

# User Interface: Metadata Export for IdPs

IdP operators choose to **opt-out** of metadata export:

## Metadata Export

If you do **not** want your IdP metadata to be included in the InCommon export aggregate, check the box below. If you leave it unchecked, *your IdP metadata will be exported by default.*

**IMPORTANT.** Once we start exporting your IdP metadata, it may be difficult to reverse that process without causing interoperability and usability issues. If you have doubts, check the box below to prevent your IdP metadata from being included in the export aggregate.

**NOTE.** Review the effect of your currently configured attribute release rules in the presence of global SP metadata. If necessary, [use the Registered By InCommon Category](#) to adjust your attribute release policy.

Do **not** include this IdP metadata in the InCommon export aggregate

Questions? Visit our wiki for a complete metadata export FAQ: [URL]



OCTOBER 4-7 · CLEVELAND OH



# eduGAIN Checklist

The rest of this presentation outlines how to prepare for eduGAIN.

1. eduGAIN for Organizations
2. eduGAIN for IdP Operators
3. eduGAIN for SP Owners



OCTOBER 4-7 CLEVELAND OH

# eduGAIN for Organizations

Are all stakeholders in your organization ready for eduGAIN?

1. Fill all [organizational roles](#) ASAP
  - a. Appoint an Executive
  - b. Identify two Federation Site Administrators
2. Read the [eduGAIN Intent Statement](#)
3. Review the new InCommon Participation Agreement (when it becomes available)



OCTOBER 4-7 CLEVELAND OH

# eduGAIN for IdP Operators

Is your IdP deployment ready for eduGAIN?

1. Configure your IdP software
2. Fine-tune your IdP metadata
3. Upgrade to Shibboleth IdP V3 (if applicable)



OCTOBER 4-7 CLEVELAND OH

# Configure your IdP Software

Complete the following tasks before Ops begins importing eduGAIN metadata:

1. Refresh and verify InCommon metadata at least daily
  - a. [Metadata Consumption](#)
  - b. [Hide From Discovery Category](#)
2. Review your attribute release policy rules
  - a. Do not rely on the md:EntitiesDescriptor/@Name XML attribute in InCommon metadata
  - b. Review your [Default Attribute Release](#) policy
  - c. Support the global Research & Scholarship Category
    - i. [Research and Scholarship for IdPs](#) (new R&S IdPs)
    - ii. [Migrating an IdP to Global Research and Scholarship](#) (existing R&S IdPs)
    - iii. Do not rely on the incommon.org R&S entity attribute value in SP metadata
  - d. [Using the Registered By InCommon Category](#)



OCTOBER 4-7 · CLEVELAND OH

# User Interface: Metadata Refresh for IdPs

IdPs confirm that they automatically refresh and verify metadata:

## Metadata Refresh

Check all that apply:

- This IdP automatically refreshes InCommon metadata, either dynamically or at least daily in batch mode*
  - This IdP verifies the signature on metadata at every refresh*
  - This IdP validates the expiration date on metadata at every refresh*

**WARNING.** An IdP that does not automatically refresh InCommon metadata should self-assert membership in the [Hide From Discovery Category](#). Otherwise the `hide-from-discovery` entity attribute may be inserted into your metadata at the discretion of InCommon Operations.

Questions? Visit our wiki to find out more about [Metadata Consumption](#).



OCTOBER 4-7 · CLEVELAND OH

# User Interface: Hide From Discovery Category

IdPs that don't automatically refresh metadata should self-assert membership in the Hide From Discovery Category:

## Hide From Discovery

If you do **not** want your IdP to appear on discovery interfaces, check the box below. If you leave it unchecked, *your IdP will appear on discovery interfaces by default.*

*Do **not** show this IdP on discovery interfaces by default*

**WARNING.** If your IdP is found to be inoperable, the `hide-from-discovery` entity attribute may be inserted into your metadata at the discretion of InCommon Operations.

Questions? Visit our wiki to find out more about the [Hide From Discovery Category](#).

# User Interface: Research & Scholarship for IdPs

An IdP declares its level of support for Research & Scholarship:

## Research & Scholarship

**Stop!** Before clicking one of the buttons below, complete at least the following steps:

1. [Configure your IdP](#) to release the [R&S attribute bundle](#)
2. [Tell us about your IdP deployment](#) by submitting a short form

Once that's done, click the appropriate button below and submit the metadata to have the R&S entity attribute inserted into metadata.

- This IdP releases the R&S Attribute Bundle to all R&S SPs globally (**recommended**)*
- This IdP releases the R&S Attribute Bundle to all R&S SPs registered by InCommon*
- This IdP does **not** support R&S*

Questions? Visit our wiki to find out more about [Research & Scholarship for IdPs](#).

# Fine-tune your IdP Metadata

Complete the following tasks before Ops exports your IdP metadata to eduGAIN:

1. Stabilize metadata elements: entityID, Scope, endpoint locations
2. Publish long-lived, self-signed [X.509 Certificates in Metadata](#)
  - a. Remove unnecessary certificates from IdP metadata
3. Publish a SAML2 SingleSignOnService endpoint that supports HTTP-Redirect binding
  - a. SAML1-only IdPs will **not** be exported to eduGAIN by default
4. Advertise support for the front-channel SSO protocols only (if possible)
  - a. Avoid advertising support for [Back-channel SAML Protocols](#)
5. Publish technical and administrative [Contacts in Metadata](#)



OCTOBER 4-7 · CLEVELAND OH



# Upgrade to Shibboleth IdP V3

As of September 26, 2015:

- 412 InCommon IdPs
  - 39 Non-Shibboleth IdP deployments
  - 373 Shibboleth IdP deployments

## Upgrading to Shibboleth IdP V3:

1. **Goal:** Deploy a test instance of Shibboleth IdP V3 by the end of 2015
2. Allocate at least 1024MB heap in the JVM
3. Point your test IdP at the InCommon Preview Aggregate
4. Know your SP partners

(as of 2015-09-26)	# of IdPs
<i>Shib IdP V1:</i>	7
<i>Shib IdP V2:</i>	318
<i>Shib IdP V3:</i>	27
<i>Shib IdP V?:</i>	21
<i>Total Shib IdPs:</i>	373



OCTOBER 4-7 CLEVELAND OH

# eduGAIN for SP Owners

Is your SP deployment ready for eduGAIN?

1. Configure your SP software
2. Fine-tune your SP metadata
3. Consolidate your SP metadata
4. Apply for membership in the Research & Scholarship Category (if applicable)



OCTOBER 4-7 CLEVELAND OH

# Configure your SP Software

Complete the following tasks before Ops begins importing eduGAIN metadata:

1. Refresh and verify InCommon metadata at least daily
2. Filter IdPs tagged with the hide-from-discovery entity attribute
  - a. If your SP has a dynamic discovery interface, do not expose such IdPs
3. Filter global metadata (only if absolutely necessary)
  - a. If you do not export your SP metadata, and your SP has a dynamic discovery interface, then you should filter global metadata up front
  - b. [Using the Registered By InCommon Category](#)



OCTOBER 4-7 CLEVELAND OH

# User Interface: Metadata Refresh for SPs

SPs confirm that they automatically refresh and verify metadata:

## Metadata Refresh

Check all that apply:

- This SP automatically refreshes InCommon metadata, either dynamically or at least daily in batch mode*
  - This SP verifies the signature on metadata at every refresh*
  - This SP validates the expiration date on metadata at every refresh*

Questions? Visit our wiki to find out more about [Metadata Consumption](#).



OCTOBER 4-7 CLEVELAND OH

# Fine-tune your SP Metadata

Complete the following tasks before Ops exports your SP metadata to eduGAIN:

1. Stabilize the SP entityID
2. Publish a human-readable DisplayName
3. Publish long-lived, self-signed [X.509 Certificates in Metadata](#)
  - a. Remove unnecessary certificates from SP metadata
4. Publish at least one SAML2 AssertionConsumerService endpoint that supports the HTTP-POST binding
5. Publish [Requested Attribute](#) elements in metadata
6. Publish technical and administrative [Contacts in Metadata](#)

**TIP.** Take advantage of [Delegated Administration](#) of SP metadata



OCTOBER 4-7 CLEVELAND OH

# Consolidate your SP Metadata

- Do you publish your metadata across multiple federations?
  - In fact, about 70 InCommon SPs publish their metadata in other federations
- If the answer is yes, eduGAIN will give you pause for thought...
  - From an operational point of view, a single source of globally distributed metadata is optimal
  - Once eduGAIN is fully operational, you may want to consolidate your metadata within a single “home federation”
- Begin the process of synchronizing disparate metadata sources so that they are functionally equivalent across federations
  - Only then can you phase out redundant metadata instances without loss of service



OCTOBER 4-7 · CLEVELAND OH

# Apply for Membership in the R&S Category

- Is your service eligible for membership in the global Research & Scholarship Category?
  - Is your service operated for the purposes of supporting research and scholarship interaction, collaboration or management, at least in part?
  - Refer to the [REFEDS Research & Scholarship Entity Category specification](#)
- [Research and Scholarship for SPs](#)
- [Research and Scholarship Application Form](#)



OCTOBER 4-7 CLEVELAND OH

# User Interface: Research & Scholarship for SPs

An SP conforms to the requirements of global Research & Scholarship:

## Research & Scholarship

**Stop!** Before checking the box below, ask the owner of this SP to [submit the R&S application form](#).

**TIP.** Make the SP owner a [delegated administrator](#) for this SP.

Once the application for R&S is approved, the delegated administrator (or a site administrator) checks the box below and submits the metadata to have the R&S entity attribute inserted into metadata.

*This SP satisfies the requirements of the [R&S Entity Category specification](#)*

Questions? Visit our wiki to find out more about [Research & Scholarship for SPs](#).



OCTOBER 4-7 · CLEVELAND OH





**2015**  
**TECHNOLOGY**  
**exchange**

**OCTOBER 4-7**  
**CLEVELAND OH**

**FEDERATION INTEROP AND EDUGAIN BRIEFING**

**Walter Hoehn, U. Memphis / Nick Roy and Tom Scavo, InCommon**