National Institutes of Health and Identity Management Requirements

IAM Online

Wednesday, April 14, 2021

Presenters:

Ann West, InCommon/Internet2

Jeff Erickson, National Institutes of Health

Brett Bieber, University of Nebraska and InCommon Assured Access Working Group

Agenda and Speakers

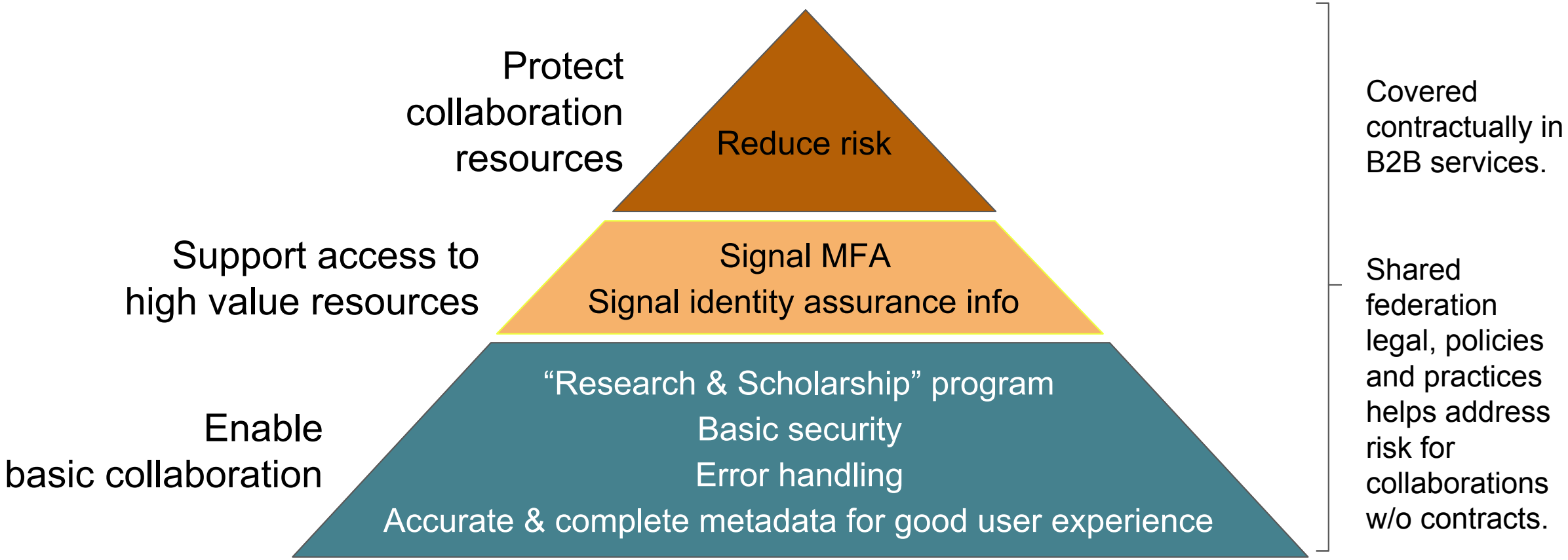
1. InCommon Federation Context
2. NIH - Why Now and What to Do
3. Recommendations for Campuses

InCommon Federation Context

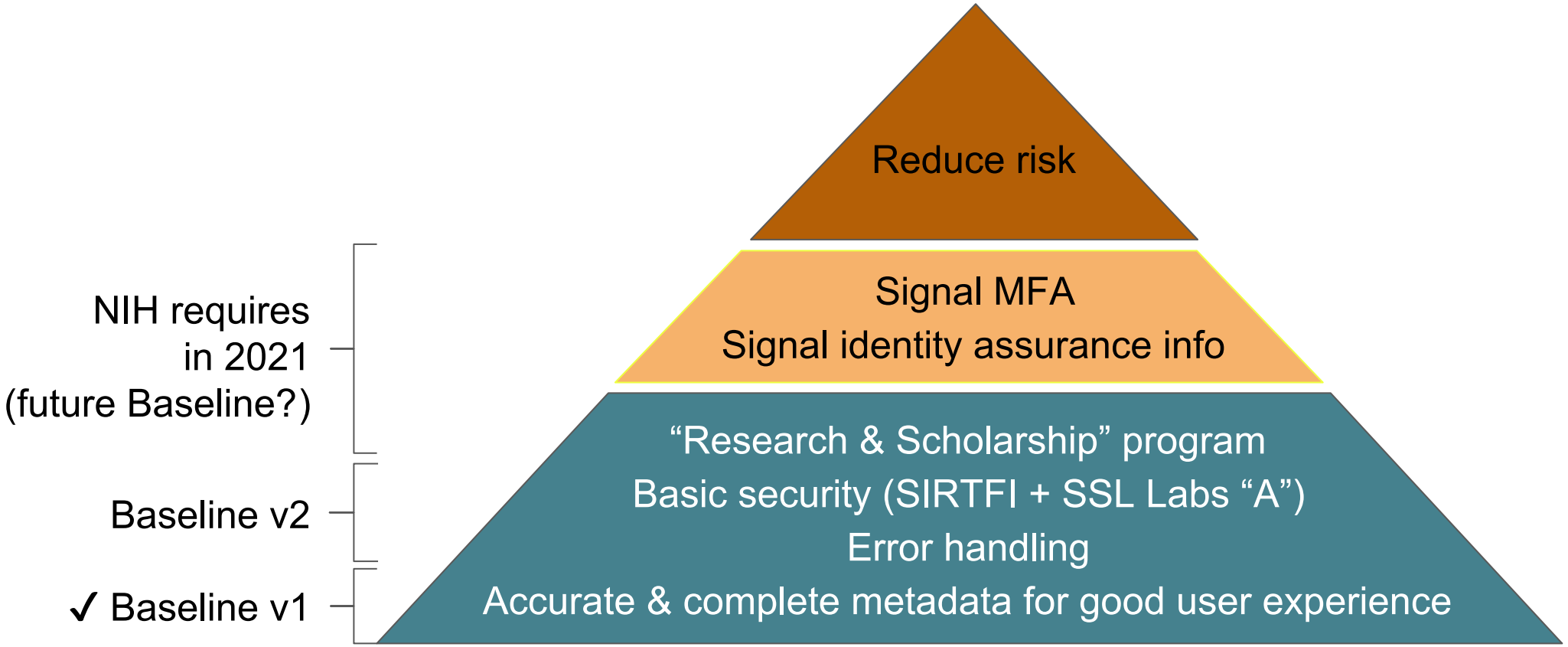
InCommon was established to support three key use cases:

- Institutional access to Library Resources
- Institutional member access to Enterprise Services
- Researcher and Scholar access to Academic Collaborations

Federation support of scholarly communities



Baseline Expectations vs NIH Requirements



NATIONAL INSTITUTES OF HEALTH
NEW IDENTITY MANAGEMENT REQUIREMENTS

Jeff Erickson

April 14, 2021

Start With Why

NIH's mission is “to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability.”

To facilitate secure access to NIH IT resources by biomedical researchers, faculty, and scientists— including controlled-access research data and grants administration systems— NIH needs:

1. Basic information about the people accessing NIH resources so that we can provision and manage efficient and secure access.
2. Strong multi-factor authentication (MFA) for all access to NIH IT resources so that we can minimize risk.
3. Assurance that the person logging in is who they say they are so that we can provide appropriate authorization to access NIH data.

What's Happening

- **Phase I** – Beginning September 15, 2021, NIH will:
  - **Signal** what is required for access
    - Federated partners need to be able to interpret and correctly respond to this signal
  - **Require** basic user information and MFA
    - **Basic information** = persistent unique identifier, name, email, affiliation, i.e., REFEDS Research and Scholarship
    - **MFA** will be required for login to
      - The **NIH electronic Research Administration (eRA) systems** including the following modules:
        - eRA Commons
        - ASSIST
        - Internet Assisted Review (IAR)
        - Commons Mobile
      - Systems that host NIH controlled-access research data
  - **Accept** federated partner's assurance of user's identity
    - REFEDS Assurance Framework v1

Note: Faculty, researchers and scientists from institutions that 1) can't interpret the NIH signal, 2) don't support the REFEDS baseline and/or 3) don't support MFA must obtain and use credentials from Login.gov

- **Phase II** – By late 2022, NIH will leverage enhancements to the REFEDS Assurance Framework
  - Allows time for federated partners to align policies and procedures with updates to the REFEDS Assurance Framework related to assertions about identity assurance

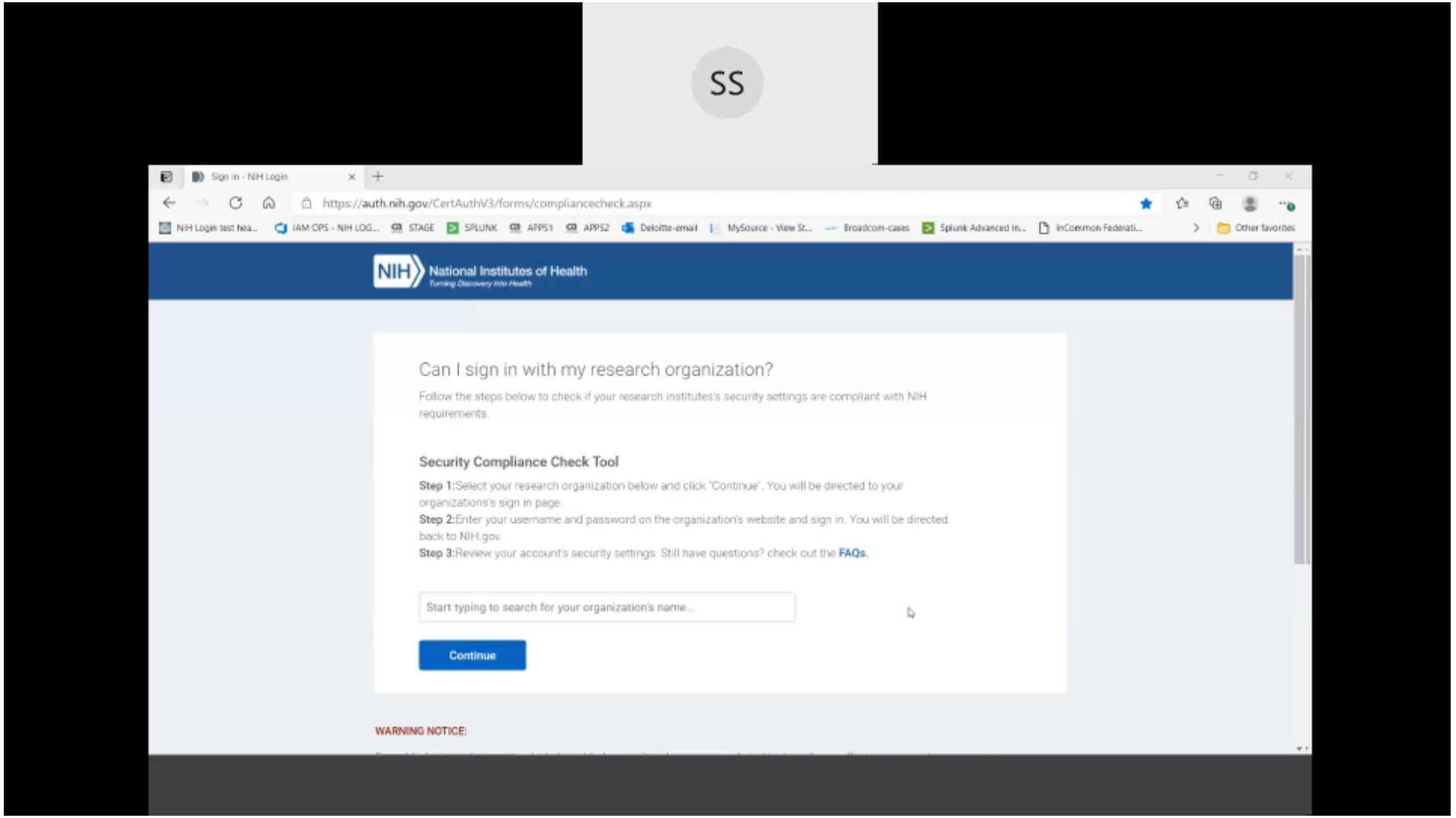
The Experience – Step by step

1. Federated user connects to URL of NIH system
2. Federated user selects their research organization from the NIH Where Are You From (WAYF) list
3. NIH signals selected IdP with request for basic information and MFA
4. IdP prompts the user for MFA
5. IdP sends NIH:
   - Basic information (REFEDS Research and Scholarship)
   - MFA assertion
   - Identity assurance
6. NIH grants access to NIH system

Test URL for IdP admins to confirm readiness:

https://auth.nih.gov/CertAuthV3/forms/compliancecheck.aspx

The Experience – What it looks like



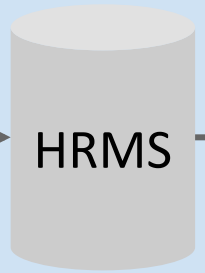
What to do!?

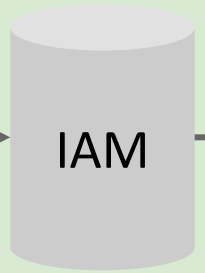
For IAM practitioners:

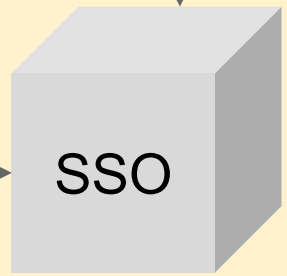
- Guidance from: Assured Access and REFEDS MFA Working Groups
- Overview of the technical connections
- Begin identifying team members and project plan

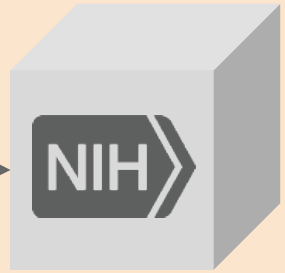
Researcher

Government Issued
Photo-ID









HR / Card Offices

Systems of Record

IAM Systems

Single-Sign-On

Service Provider

Researcher

Government Issued
Photo-ID

HRMS

IAM

SSO

R&S Entity Category SP

In-Person or
Remote Proofing

Name
I9 or E-Verify Date

Identifier(s)
Authenticators
Assurance Levels

Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

HR / Card Offices

Systems of Record

IAM Systems

Single-Sign-On

Service Provider

Researcher

Government Issued
Photo-ID

In-Person or
Remote Proofing

HR / Card Offices

HRMS

Name
I9 or E-Verify Date

Systems of Record

IAM

Identifier(s)
Authenticators
Assurance Levels

IAM Systems

SSO

Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

Single-Sign-On

R&S Entity Category SP

Service Provider

Researcher

Government Issued
Photo-ID

HRMS

IAM

SSO

R&S Entity Category SP

In-Person or
Remote Proofing

Name
I9 or E-Verify Date

Identifier(s)
Authenticators
Assurance Levels

Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

HR / Card Offices

Systems of Record

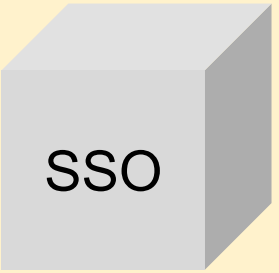
IAM Systems

Single-Sign-On

Service Provider

Researcher

Government Issued
Photo-ID



R&S Entity Category SP

In-Person or
Remote Proofing

Name
I9 or E-Verify Date

Identifier(s)
Authenticators
Assurance Levels

Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

Single-Sign-On

HR / Card Offices

Systems of Record

IAM Systems

Service Provider

Researcher

Government Issued
Photo-ID

HRMS

IAM

SSO

In-Person or
Remote Proofing

Name
I9 or E-Verify Date

Identifier(s)
Authenticators
Assurance Levels

Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

HR / Card Offices

Systems of Record

IAM Systems

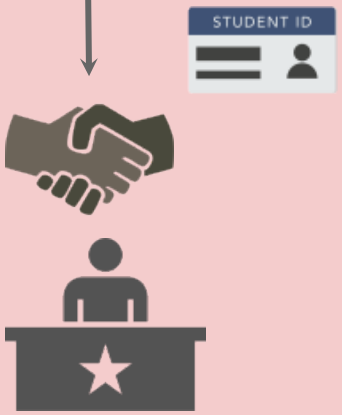
Single-Sign-On

R&S Entity Category SP

Service Provider

Researcher

Government Issued
Photo-ID



In-Person or
Remote Proofing

HR / Card Offices

HRMS

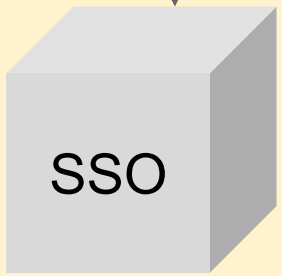
Name
I9 or E-Verify Date

IAM

Identifier(s)
Authenticators
Assurance Levels

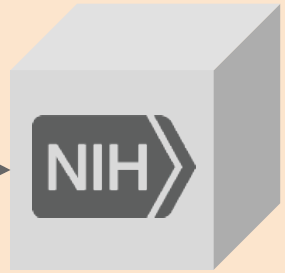
Systems of Record

IAM Systems



Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

Single-Sign-On

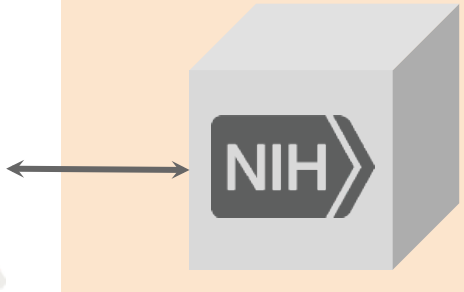


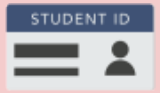
R&S Entity Category SP

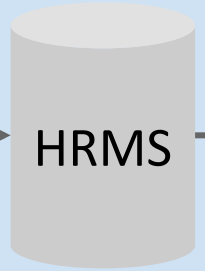
Service Provider

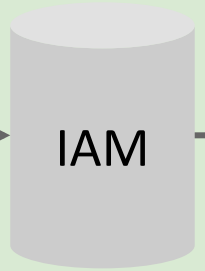
Researcher

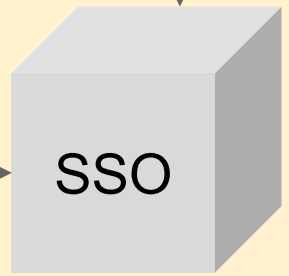
Government Issued
Photo-ID











In-Person or
Remote Proofing

Name
I9 or E-Verify Date

Identifier(s)
Authenticators
Assurance Levels

Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

R&S Entity Category SP

HR / Card Offices

Systems of Record

IAM Systems

Single-Sign-On

Service Provider

REFEDS Assurance Framework IAP Levels

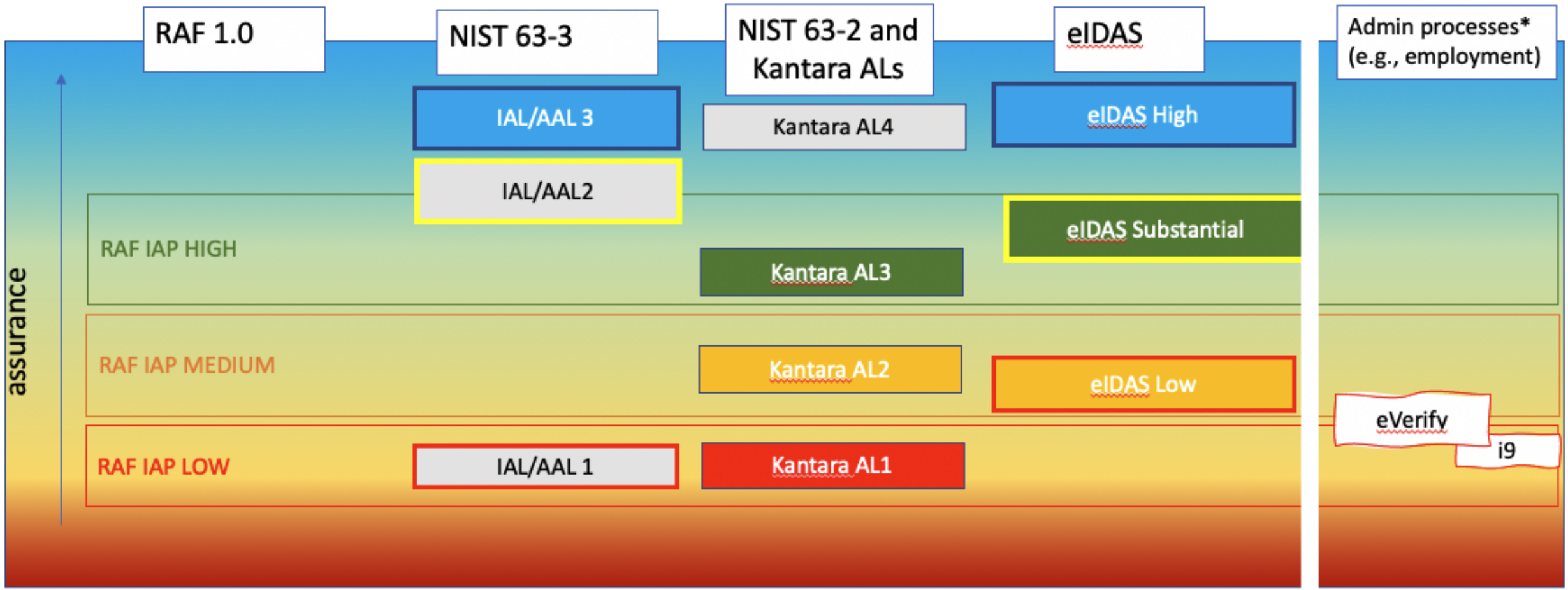
Claim levels:

- local-enterprise

- low
- medium
- high

Assurance Spectrum

Different frameworks' tiers are not equivalent (e.g., RAF Medium is eIDAS Low)



*Note: Admin processes must be institutionally linked to network credential issuance. If they are not, the assurance is lost.

The NIH Phase I Ask

NIH needs your help to facilitate secure access by researchers in your organizations to NIH systems and data, including controlled-access data.

By September 15, 2021, we ask that you:

1. Adopt the REFEDS Research and Scholarship Entity Category (R&S)
    a. Signal a standard set of basic, non-sensitive information (persistent unique identifier, name, email + affiliation)

2. Adopt the REFEDS MFA profile (https://refeds.org/profile/mfa)
    a. Signal your assurance of strong authentication (MFA)

3. Adopt the REFEDS Assurance Framework v1
    a. Signal your assurance of the person's identity (at min. "Local Enterprise")

Recommended Next Steps

- As soon as possible, research organizations should use the NIH test URL to confirm their readiness to receive and respond to signals for the REFEDS MFA and Assurance Framework:
  - Test URL is https://auth.nih.gov/CertAuthV3/forms/compliancecheck.aspx
    - Confirm IdP can receive and process NIH signal
    - Confirm IdP can perform MFA
    - Confirm IdP can respond with required information (basic user information, MFA claim, and identity assurance)
  - Key target dates:
    - **June 2021:** NIH will start accepting compliant assertions from federated research organizations to access eRA and other applications
    - **September 2021**: NIH will require MFA to access eRA
- Before December 2022:
  - Plan how to implement identity assurance claims
  - Assess where identity proofing occurs
  - Assess critical groups not covered
  - Update policies and procedures to address gaps

Where to get more information

Get the latest: News on NIH-requested InCommon Identity Provider changes:

Get NIH Ready - InCommon Federation - Internet2 Wiki

In Action: These groups are working on specific guidance for signaling the REFEDS MFA and Identity Assurance Framework profiles

InCommon Assured Access Working Group

REFEDS MFA Group - Visit the REFEDS Assurance Working Group wiki for the latest

Where to get more information

REFEDS Specifications and Working Groups

REFEDS MFA Profile
https://refeds.org/profile/mfa

REFEDS Assurance Framework
https://refeds.org/assurance

REFEDS Research and Scholarship Category
https://refeds.org/research-and-scholarship

REFEDS Assurance Working Group
https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group

NIH Announcements and Resources

eRA to Require Two-Factor Authentication
https://era.nih.gov/register-accounts/access-era-modules-via-login-gov.htm#Federated_Users

NIH Security Compliance Check Tool
https://auth.nih.gov/CertAuthV3/forms/eRAcompliancecheck.aspx

NCBI (PubMed) adopting federated credentials
https://ncbiinsights.ncbi.nlm.nih.gov/2021/01/05/important-changes-ncbi-accounts-2021/

NIH Login Services
https://auth.nih.gov/docs/

IAM Online Evaluation

https://www.surveymonkey.com/r/IAMOnline-Apr-2021

- For those new to identity and access management, federation, and/or the InCommon Trusted Access Platform
- Held online Noon - 4:30 ET daily - July 12-16, 2021
- View the web page for [program and registration information]

- The Call for Proposals for CAMP is open through April 30, 2021
- Held online partial days
  - CAMP - October 4-5 (case studies, organizational practices in IAM)
  - Advance CAMP - October 6-8 (unconference - moving IAM forward globally
- View the web page for information on submitting a proposal and registration