

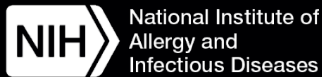
National Institute of Allergy and Infectious Diseases

NIH, NIAID and REFEDS

NIH adoption of REFEDS MFA Profile and REFEDS Assurance Framework

NIAID's implementation of REFEDS Assurance Framework at ICERs Mali and Uganda

NIAID



Kyle Lewis
NIAID IBRSP International Team ISSO

Agenda

- Introduction to REFEDS profiles
- NIH new requirements – What changed?
- Overview of REFEDS Assurance Framework's Identity Assurance Profiles
 - Service Provider Perspective (e.g., NIH, eRA Commons)
 - Identity Provider Perspective (your institutions, NIAID ICERs)
- Summary

Context:

What is REFEDS MFA and RAF?

- REFEDS: Research and Education Federations Group
 - Articulates mutual needs of research and education identity federations world-wide
- REFEDS MFA Profile
 - A way for IdPs to signal credential assurance (e.g., Multi-Factor Authentication) for their users to Service Providers
 - “How sure am I that these credentials are not compromised?”
- REFEDS Assurance Framework (RAF)
 - A way for IdPs to signal identity assurance for their users to Service Providers
 - “How sure am I that the person to whom I issued network credentials is the person they claimed to be?”

What Changed | Phase 1

Phase 1 — November 2020 to September 15, 2021 — laid the foundation for a new standard of federated login to NIH systems and sites, starting with the NIH Electronic Research Administration (eRA) system.

1. **NIH signals** what is required for access
 - Federated partners need to be able to interpret and correctly respond to this signal
2. **NIH requires basic user information** including persistent unique identifier, name, email, and affiliation
 - This basic information equates to the [REFEDS Research and Scholarship Entity Category \(R&S\)](#)
3. **NIH requires MFA** (using the [REFEDS MFA profile](#)) for login to the following eRA modules:
 - eRA Commons
 - ASSIST
 - Internet Assisted Review (IAR)
 - Commons Mobile

Are you ready for NIH Phase 1? Use the eRA Security Compliance Check Tool to find out:
<https://auth.nih.gov/CertAuthV3/forms/eRAcompliancecheck.aspx>

Note: For now, 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 *may* be able to log into eRA using their existing eRA credentials (i.e., no federated access). As eRA moves forward with their rollout of MFA, those researchers must obtain and use credentials from [Login.gov](#).

Phase 2 Compliant?

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

By December 2022:

- ✓ **Accept** the NIH signal for a standard set of basic, non-sensitive information (persistent unique identifier, name, email + affiliation)
 - Adopt the [REFEDS Research and Scholarship Entity Category \(R&S\)](#)
- ✓ **Signal** your assurance of strong authentication (MFA)
 - Adopt the [REFEDS MFA profile](#)
- Signal** your assurance of the person's identity
 - Adopt the [REFEDS Assurance Framework v1](#)

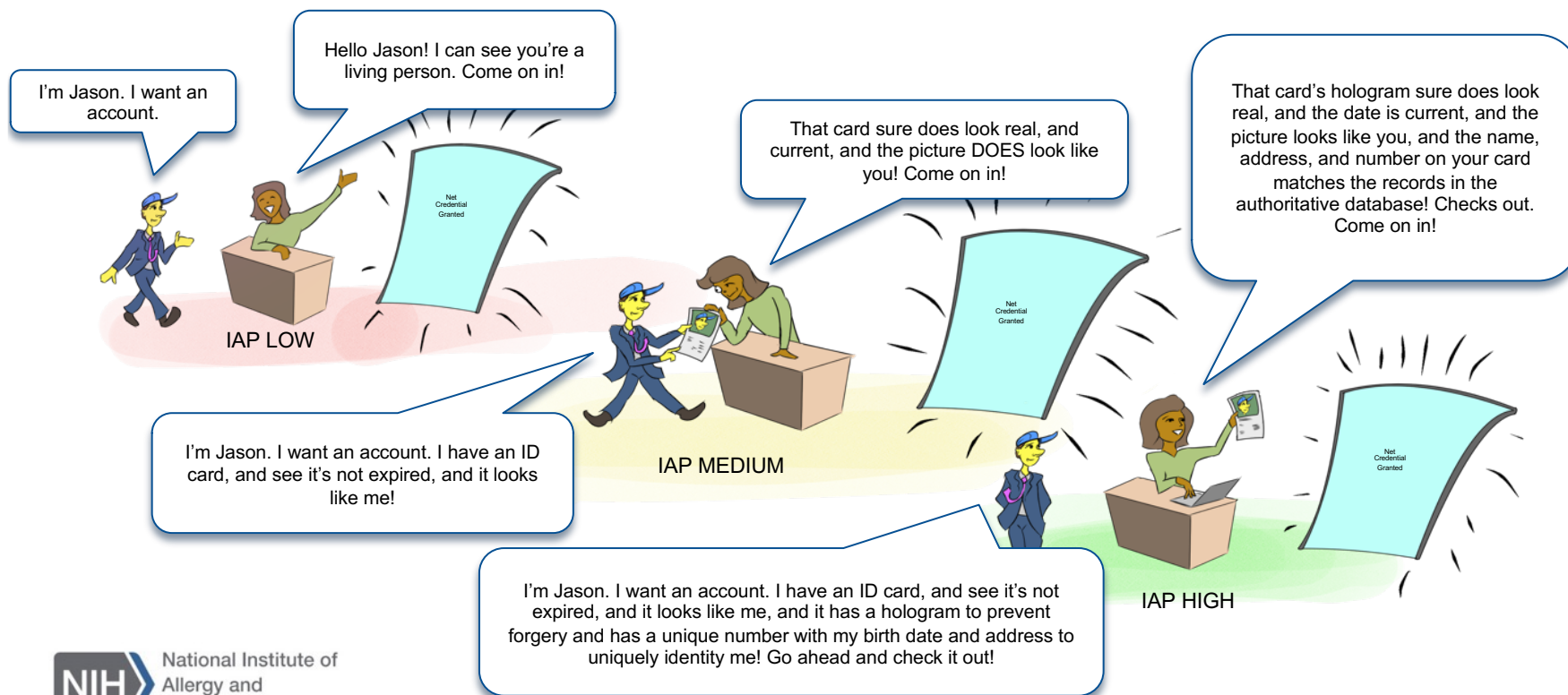
Are you ready for NIH Phase 2? Use the NIH Security Compliance Check Tool to find out:
<https://auth.nih.gov/CertAuthV3/forms/compliancecheck.aspx>

Users will need to authenticate via Login.gov if organizations are not compliant

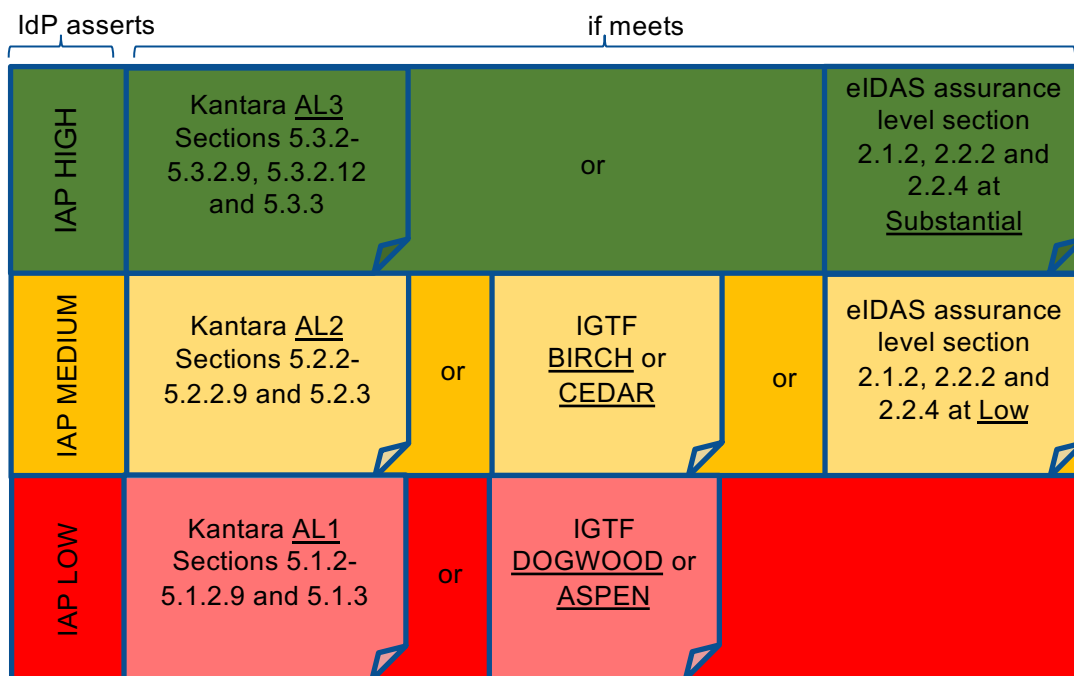
 **LOGIN.GOV**

REFEDS Assurance Framework

Illustrated IAPs Examples

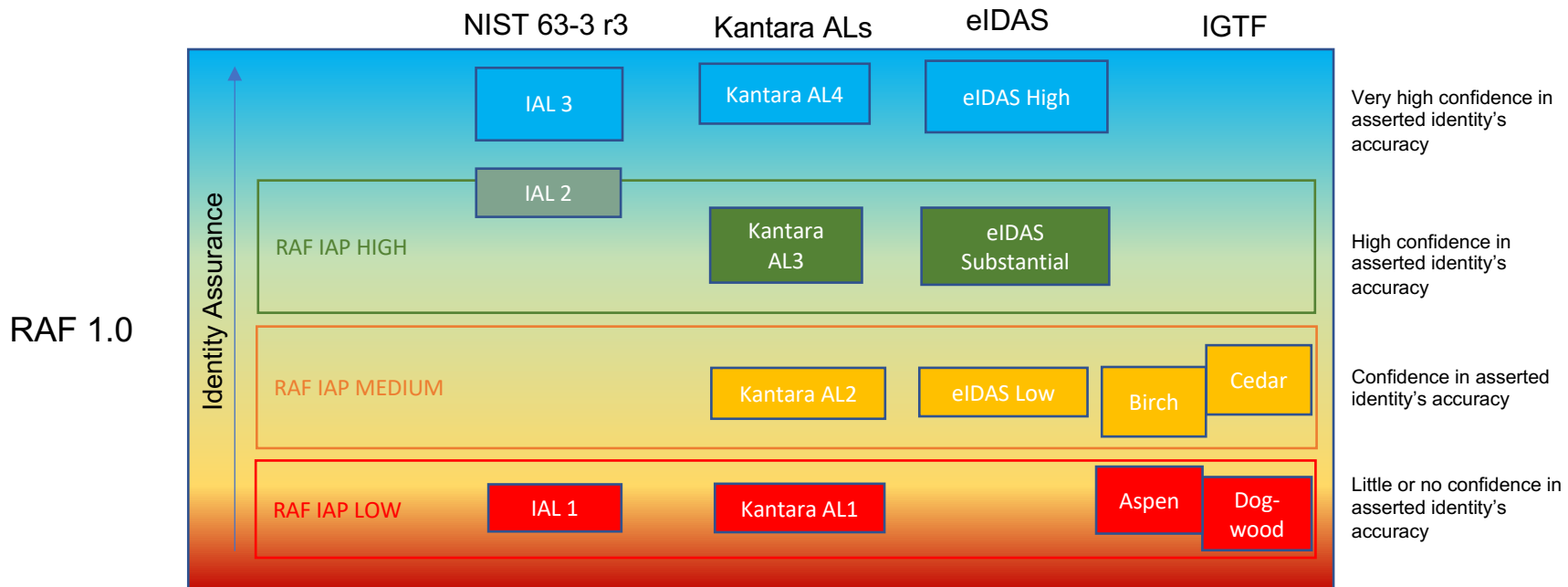


REFEDS Assurance Framework 1.0 Based on Disparate International Systems

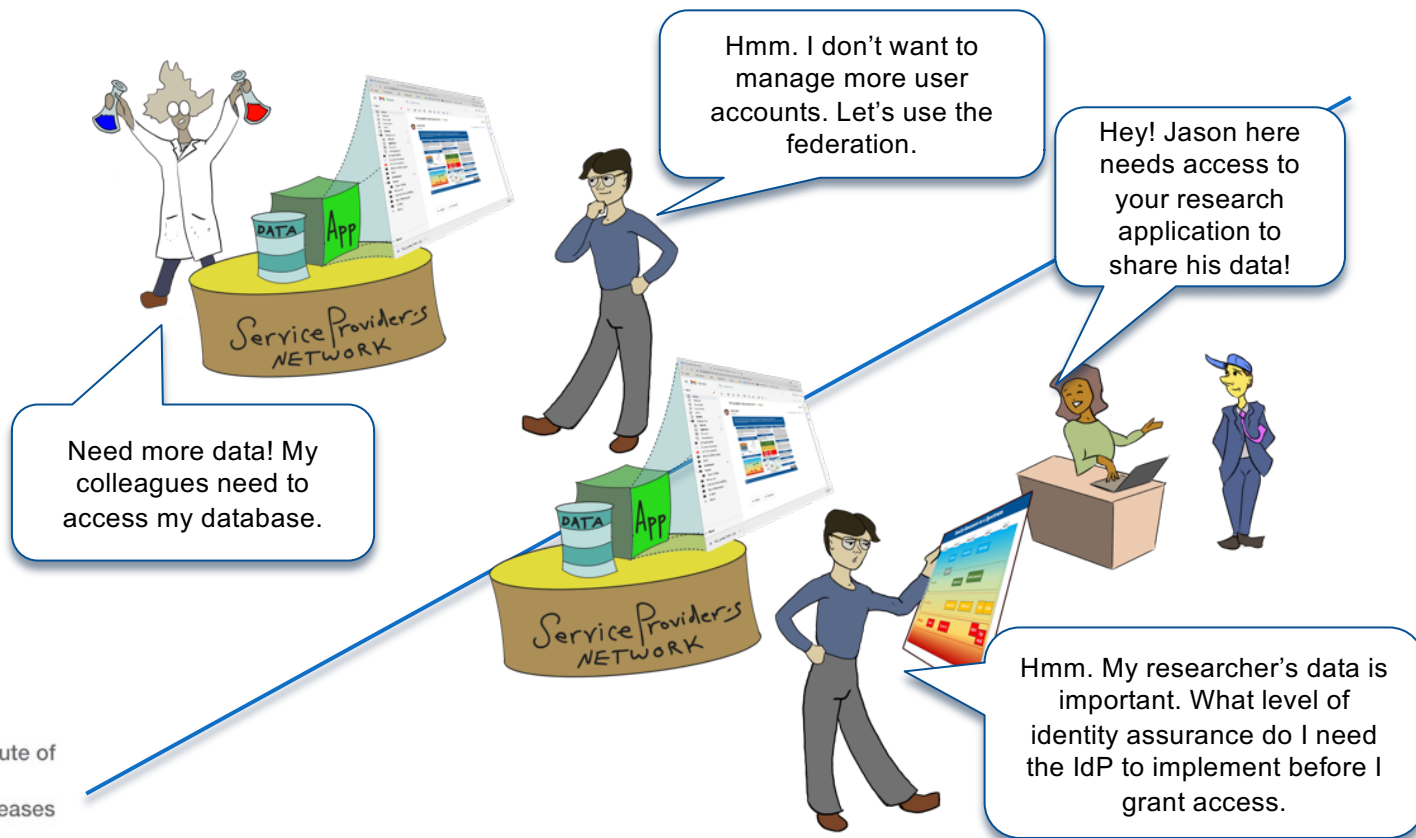


- Kantara Assurance Levels (ALs) = adaptation of deprecated U.S. NIST 800-63-2
- IGTF = Interoperable Global Trust Federation
- eIDAS = European Union standards and guidance

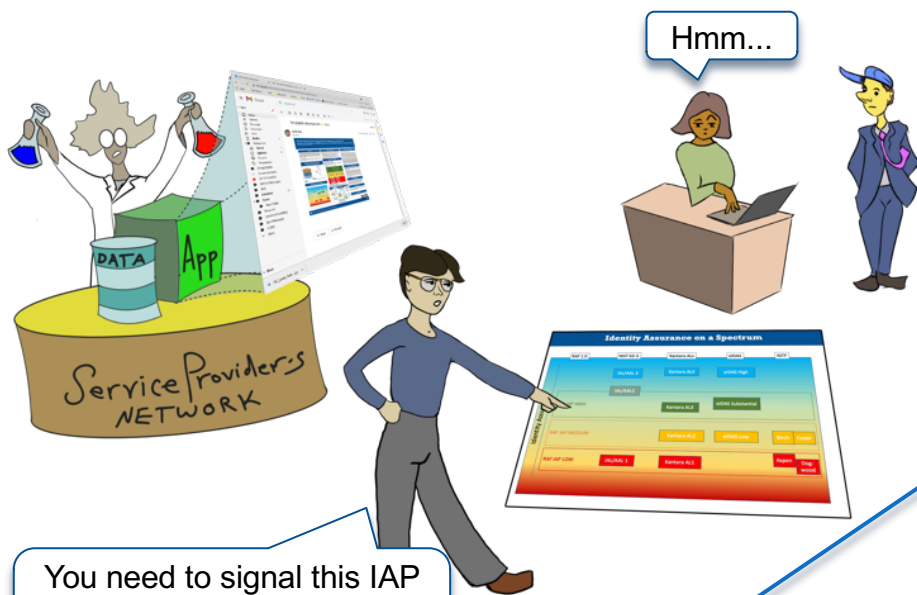
Analyzing RAF vs Other Frameworks



Service Provider's Perspective

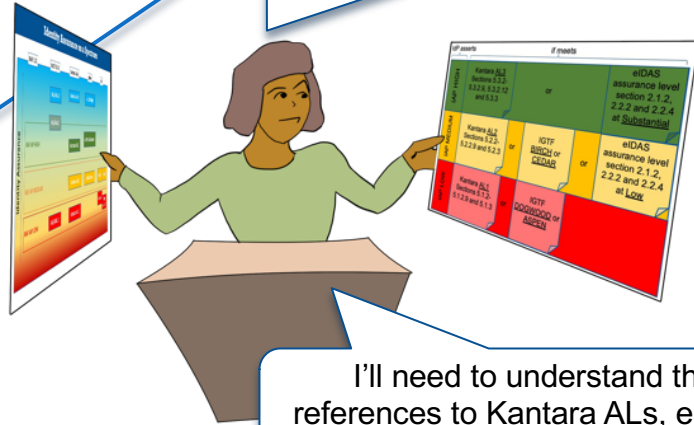


Identity Provider's Perspective



I need to figure out if my user registration process is sufficient, or what's needed to meet the required IAP!

You need to signal this IAP before I let your user in to my application.



I'll need to understand the references to Kantara ALs, eIDAS, or IGTF.

NIAID ICER Implementation (Mali and Uganda)

NIAID IBRSP implemented in-person revalidation of all users
(we have <1000 users each location)

- Assigned “IAP High” – current Government Photo ID visually checked and cross-check with employee or student registrar
- Assigned “IAP Medium” – Government Photo ID, but without checking or validating with another authoritative source
- Assigned “IAP Low” – if person came in but documentation didn’t qualify for Medium or High
- Assigned IAP “zero” – those users who did not come to help desk to revalidate

Access decisions made (e.g., IAP “zero” restricted to email only access)

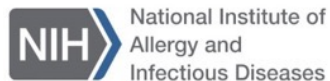
Summary

- NIH no longer issuing credentials
- If you need to access eRA Commons, you need to do so with your own institutional credentials
- If your institution cannot provide multi-factor authentication, only other option is login.gov
- Dec 2022 (target), if your institution cannot signal RAF, only other option is login.gov

Acknowledgements

- Jeff Erickson, NIH Chief of IAM
- Sumit Nanda, NIH
- Michael Tartakovsky, NIAID CIO
- Chris Whalen, Research Data and Communications Technologies
- Tom Barton, Internet 2
- Jule Ziegler, REFEDS Assurance Framework WG Chair
- Brett Bieber, InCommon Federation, Assured Access WG Chair

Questions/Discussion



Kyle Lewis (Contractor, **RDCT**)
NIAID International Biomedical Research Support Program (IBRSP)

kyle.lewis@nih.gov
kewis@researchdata.us

NIAID

REFEDS Assurance Framework | Spectrum

Identity assurance exists on a spectrum of confidence levels from low to very high confidence in the asserted identity's accuracy. **It's important to note that administrative processes such as employment must be institutionally linked to network credential issuance.** If they are not, the assurance is lost.

Identity Assurance Levels	RAF 1.0	NIST 63-3	Kantara ALs	eIDAS	IGTF	Admin Processes
Level 4 —Very high confidence in the asserted identity's accuracy		IAL3	Kantara AL4	eIDAS High		
Level 3 —High confidence in the asserted identity's accuracy	RAF IAP High	IAL2	Kantara AL3	eIDAS Substantial		
Level 2 —Confidence in the asserted identity's accuracy	RAF IAP Medium		Kantara AL2	eIDAS Low	Birch & Cedar	
Level 1 —Little or no confidence in the asserted identity's accuracy	RAF IAP Low	IAL1	Kantara AL1		Aspen & Dogwood	E-Verify & I-9