




Increasing Identity Assurance and Improving NIH Readiness

IAM Online: May 12, 2021


Brett Bieber (U of Nebraska), Chair, Assured Access Working Group

Tom Barton (UChicago/Internet2), host


Mitigating the Risk of an Authentication Failure

- 
- Authentication failure occurs when an unauthorized user accesses a protected resource using an authorized credential
 - The resource is protected for a reason - there can be negative impact if it is accessed by an unauthorized person
 - Sensitive data about human subjects
 - Scientific, legal, and logistical representations associated with grants and contracts
 - MFA mitigates the risk that a credential issued to its intended user is in fact used by another person
 - Identity assurance mitigates the risk that an unintended user can fraudulently pose as the intended one and be issued their credential

How Much Mitigation is Enough?

- 
- Two factor authentication is often accepted as strong enough to mitigate the chance that a user's credential passes out of their exclusive control
 - But colleges have much less experience with identity assurance
 - They tend to rely on the relationships people have with them (faculty, staff, student), the continued demonstration of which increases confidence in their authenticity
 - Now put federation in the picture, where the relying party has no insight into this demonstrated authenticity
 - How confident would you be in telling them not to worry? How can you express a degree of such confidence?

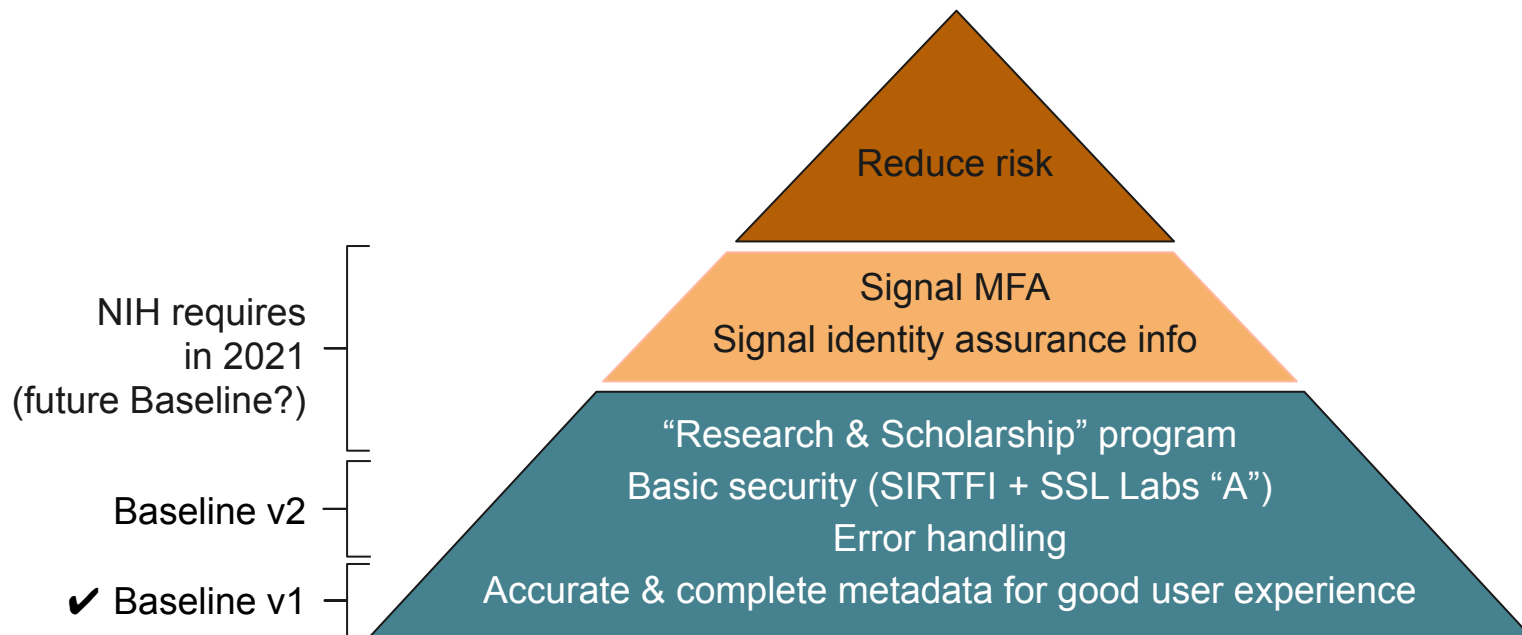
Get NIH Ready

- 
- NIH strongly supports federated access to their services - it shortens time-to-research-results that help save lives
 - But NIH must also mitigate the risk of federated authentication failure

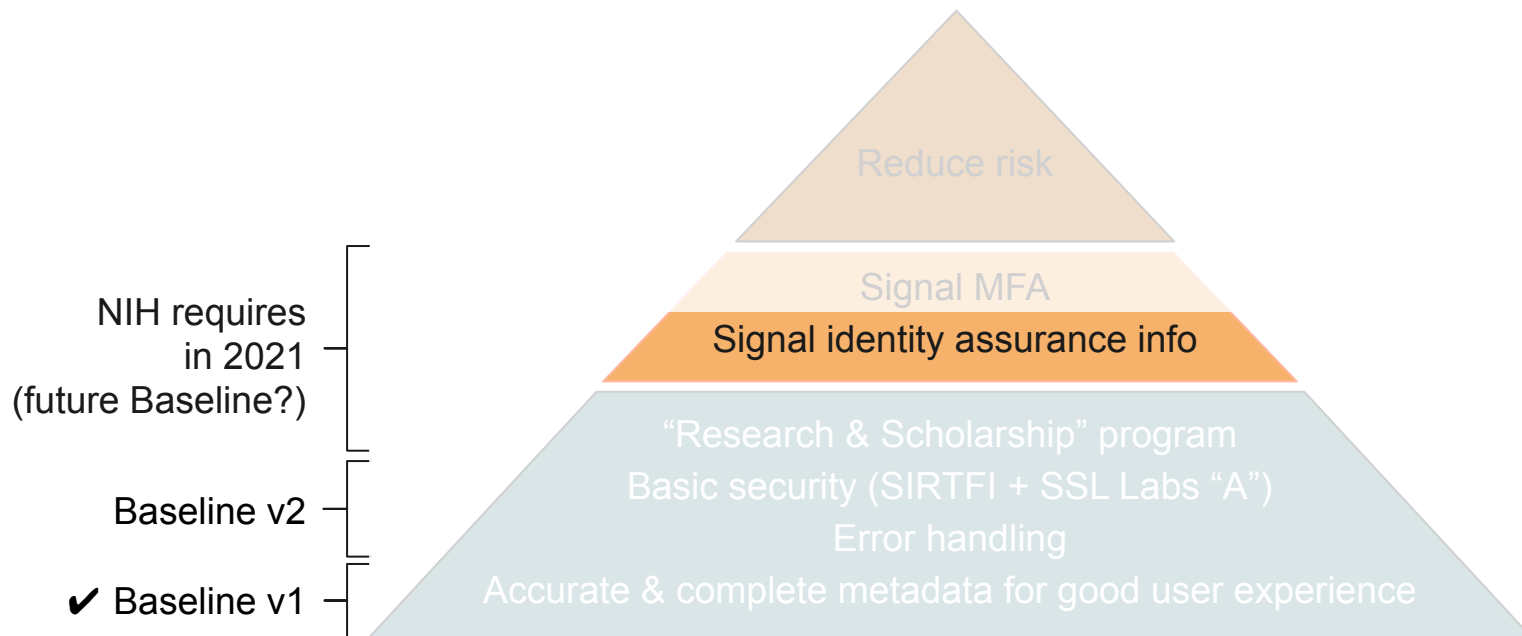
Ergo

- Two factor authentication is becoming required to access resources having corresponding risk
- So is identity assurance, but given lack of much actual experience with this form of mitigation and recognition of the risk of asking for too much too soon, its adoption will be more of a journey, with multiple steps
- Brett will show us how to take the first steps of that journey

Baseline Expectations vs NIH Requirements



Baseline Expectations vs NIH Requirements





What is Assurance Anyways!?

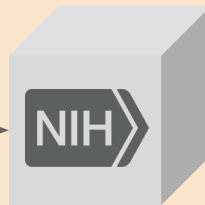
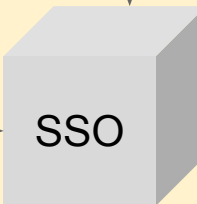
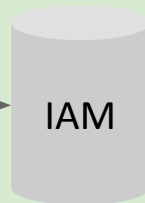
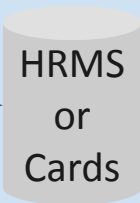
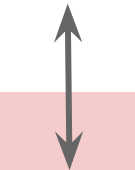
Identity assurance in the context of federated identity management is the ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity.

Source: https://en.wikipedia.org/wiki/Identity_assurance

Researcher



Government Issued
Photo-ID



HR / Card Offices

Systems of Record

IAM Systems

Single-Sign-On

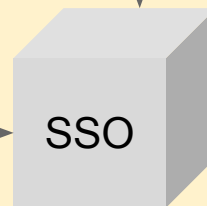
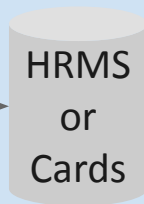
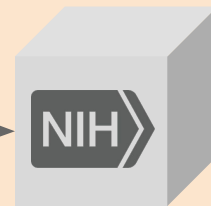
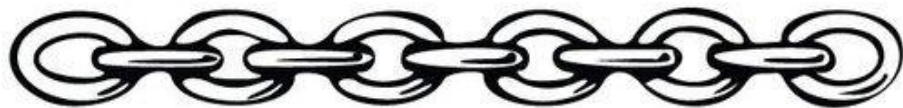
Service Provider



Researcher



brett.bieber@nebraska.edu



HR / Card Offices

Systems of Record

IAM Systems

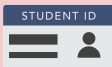
Single-Sign-On

Service Provider

Researcher

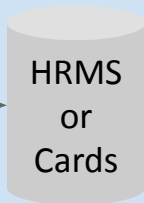


Government Issued
Photo-ID



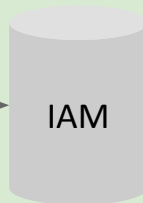
In-Person or
Remote Proofing

HR / Card Offices



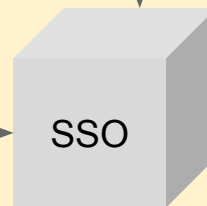
Name
I9 or E-Verify Date
ID Card

Systems of Record



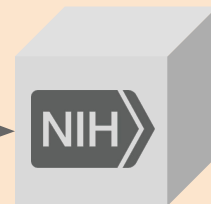
Identifier(s)
Authenticators
Assurance Levels

IAM Systems



Identifiers
Name
Email
R&S Attributes
eduPersonAssurance

Single-Sign-On



R&S Entity Category SP

Service Provider

Poll: How would you rate your level of anxiety with the NIH *Assurance* Requirements?



REFEDS Assurance Framework Implementation Guidance for the InCommon Federation

Assured Access Working Group

Quick 25 page document



1



2



3



4



5



6



7



8



9



10



11



12



13



14



15



16



17



18



19



20



21



22



23



24



25



26



REFEDS Assurance Framework

eduPersonAssurance (OID:1.3.6.1.4.1.5923.1.1.1.11)

- local-enterprise <https://refeds.org/assurance/IAP/local-enterprise>
- high <https://refeds.org/assurance/IAP/high>
- medium <https://refeds.org/assurance/IAP/medium>
- low <https://refeds.org/assurance/IAP/low>



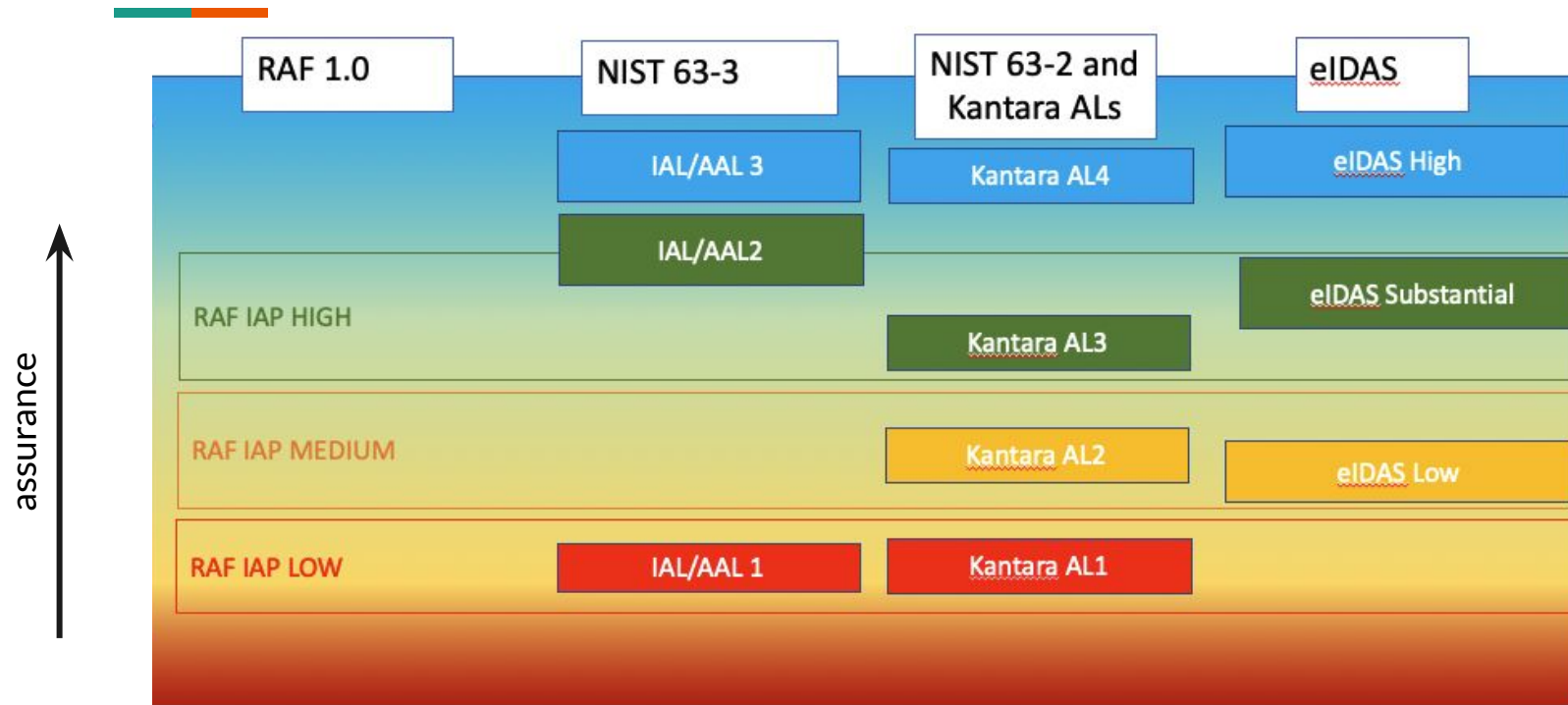
local-enterprise

“The identity proofing and credential issuance, renewal and replacement are done in a way that qualifies (or would qualify) the user to access the Home Organisation’s internal administrative systems (see appendix A).”

- Employee self-service operations, e.g. paycheck deposit

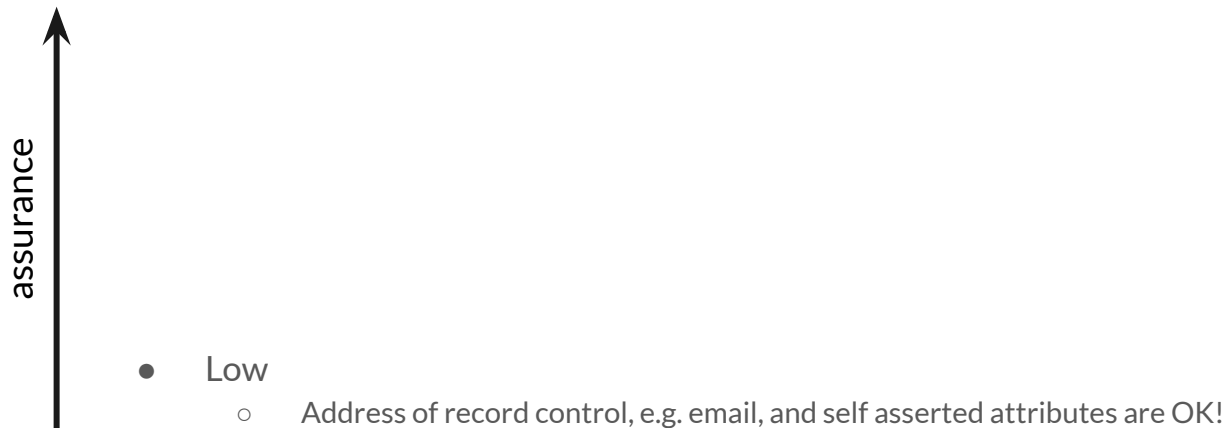
Are the processes the same for other (broader) populations? E.g. Students?

Assurance Spectrum





Claim Levels






Claim Levels

assurance ↑

- Medium
 - Government issued photo ID must be verified.
 - Ensure credentials are bound to the user
 - Password resets must ensure equivalent proofing, or re-proofing and binding of the identity to credential
 - Policies must forbid sharing of accounts and credentials
- Low
 - Address of record control, e.g. email, and self asserted attributes are OK!



Claim Levels

- 
- High
 - Verify evidences against their government source
 - Medium
 - Government issued photo ID must be verified.
 - Ensure credentials are bound to the user
 - Password resets must ensure equivalent proofing, or re-proofing and binding of the identity to credential
 - Policies must forbid sharing of accounts and credentials
 - Low
 - Address of record control, e.g. email, and self asserted attributes are OK!



Existing Processes to Leverage

- Hiring & HR
- Card Offices



Hiring & HR

Possible Levels:

- IAP/high
- IAP/medium
- IAP/low

- Form I-9
 - Only qualifies for Medium if the identity evidence was a government issued photo ID.
- E-Verify
 - Checks the data entered into the I-9 form, but does not validate the identity documents themselves.

Employee relationships may pre-date these processes



Card Offices

Possible Levels:

- IAP/medium
- IAP/low

Existing processes may be leveraged!

- Is there a documented procedure to verify non-expired government issued photo ID when the card is issued?
- Are cards assigned (in the DB) before ID is verified?



Other Processes or New Processes

- Remote Proofing
- Dedicated Identity Proofing

What do I do?



What do I do?

- ❑ Research where Identity Proofing is performed.
- ❑ Understand your scope of users and assess alignment with RAF IAP.
- ❑ Collect interested stakeholders and devise an implementation plan for the RAF claim levels.

Order of Implementation:

1. local-enterprise
2. low
3. medium
4. high



NIH Compliance Check Tool

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

Compliance Check Results



Compliant

Your research organization's security settings comply with [NIH security requirements](#).

[Show less](#)

✔ **Multi-Factor Authentication:**enabled

✔ **IAP Assurance Level:**medium

✔ **Released attributes:**First Name, Last Name, Email Address, EPPN, Organization

**Poll: Have you tried the NIH
Compliance Check Tool?**

**Poll again: How would you rate your
level of anxiety with the NIH
Assurance Requirements?**

Poll: If local-enterprise would be required in the next 3 months, could you meet that deadline?

Poll: If medium would be required in the next 3 months, could you meet that deadline?



Resources

Consultation: [REFEDS Assurance Framework Implementation Guidance for the InCommon Federation](#)

Get NIH Ready: <https://spaces.at.internet2.edu/display/federation/get-nih-ready>

InCommon Catalyst: <https://incommon.org/community/catalyst/>

IAM Online Evaluation

<https://www.surveymonkey.com/r/IAMOnline-May-2021>