What’s Up with Assurance?

Tom Barton, Internet2

FIM4R
December 2022

What's happening

Two forms of assurance:

- ***Authentication assurance***, which mostly boils down to ***Multi-Factor Authentication***
- ***Identity assurance***, eg, vetting a person's identity using government issued identity documents

- NIST SP800-63-3 standards imposed on the US Federal government by executive order are causing MFA to become required for most federal systems
  - Example: NSF & NIH grants management systems
- Identity assurance is also becoming required for FISMA Moderate systems
  - Example: NIH systems with human health data
- Similar requirements are emerging for similar European systems
- Such requirements flow down in time to many organizations in various ways

What I’m going to say

- There are several ways to address identity assurance, one or more might fit well with some research environments
- NIST and eIDAS aren’t the only assurance standards. The ***REFEDS Assurance Framework (RAF)*** can be acceptable to responsible officials.
  - ***NIH accepts RAF*** as an alternative to NIST because of their international users and suitability for universities
  - ***RAF is becoming required by some EU systems*** with human health data
- Growing number of commercial identity proofing services handle various forms of government ID (though mainly US focused?)
- Many federated Identity Providers do MFA, fewer do identity assurance yet

What’s the point of assurance?

You provide or accept credentials for which system access is authorized. What could go wrong?

System access by an unauthorized person is one way.

- Unauthorized person using an authorized credential is mitigated by ***authentication assurance (strong authentication or MFA)***
- Unauthorized person being given an authorized credential is mitigated by ***identity assurance (fraud mitigation)***

It boils down to how sure you need to be of who is accessing your system.

What’s at stake?

Ways to mitigate fraud potential

1. Prove user's identity by reference to identity documents, usually government-issued
    - User and Registrar together in person
    - User and Registrar together over video conference (supervised remote)
    - Automated, no Registrar present (unsupervised remote)

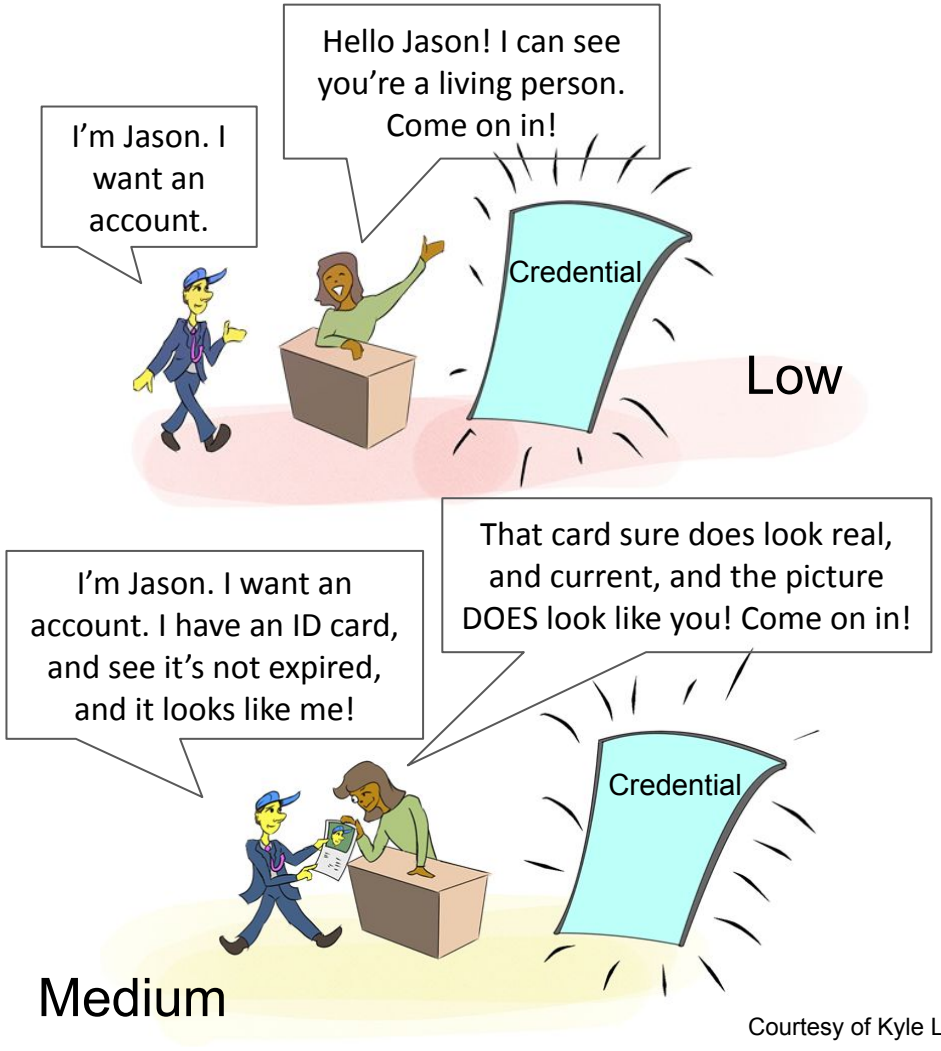
2. Prove user's identity by vouch from a trusted person

3. Prove user's identity by vouch from a trusted organization
    a. They vetted + trustworthy means of notification
    b. A different sort of vouch - user's home organization claims they trust the user to access some of their critical internal systems

Steps in identity document based vetting process

0. Define acceptable identity documents
    - Recognized sources/issuers
    - Ability to determine genuineness
1. Validate identity document(s) presented by the user
    - Check identity document security features
    - Check whether the identity presented in the identity document is known to exist
2. Verify that the user is who the identity document represents
    - Registrar's brain cells compare photo with user, or
    - Suitable technology does similar
3. Establish and maintain the binding between user's authenticator and the vetted identity

Greater diligence in doing these things yields higher identity assurance levels ie, better fraud protection



Courtesy of Kyle Lewis

Vouching by a trusted person

- ***Trusted Referee***: qualified person who can ***vouch*** for the user
  - Who's qualified and how vouching is done are determined in system context
- In some research systems, PIs or other designated project leaders can act as Trusted Referees to vouch for the identities of their team members
- A Trusted Referee may need to go through an identity document based vetting process before their vouches can be accepted
- ***Forthcoming RAF v2*** also embraces ***vouching*** as an alternative to using identity documents as the basis for identity proofing

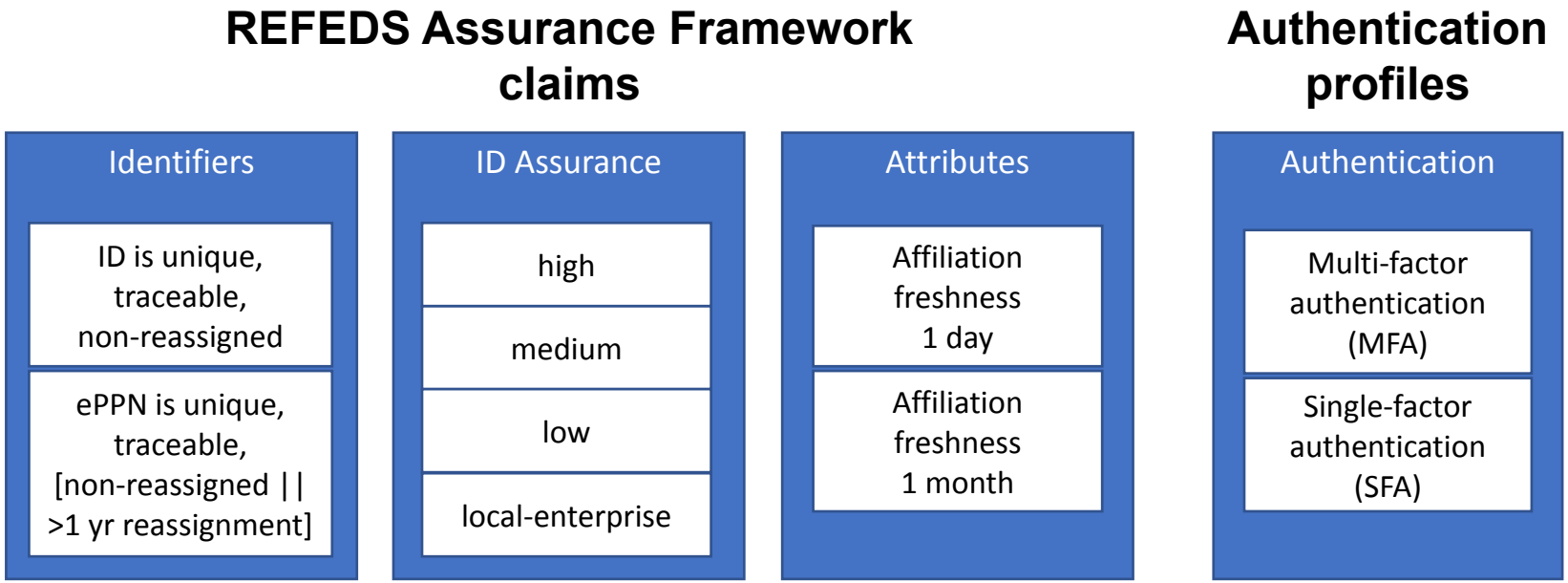
Vouching by a user's home organization

- Risk-based alternative to checking identity documents: ***RAF local-enterprise***

  Home organization asserts that they trust the user to access some of their critical internal systems
- Critical internal systems are those that …
  - manage some of the organisation's expenditures,
  - manage employment-related personal data,
  - manage student-related personal data,
  - manage some aspect of the organisation's regulatory or legal compliance obligations, or
  - are vital to the functioning of the organisation

- It's stronger than RAF low, not comparable to either medium or high
- Use if you trust the issuer and believe their "critical" is similar to your "critical"

An international assurance framework for research



https://refeds.org/assurance

Identity assurance levels compared

NIST	
IAL1	Subject is a natural person
IAL2	Substantial vetting. Supervised and unsupervised options.
IAL3	IAL2 + stricter selection of identity docs - unsupervised option

RAF v2	
low	Subject is a natural person
medium	Modest vetting. Supervised and unsupervised options.
high	~= IAL2 with less prescriptive criteria to accommodate international contexts

eIDAS	
Low	Modest vetting, identity independently known to exist
Sub-stantial	Substantial vetting. No unsupervised option.
High	Substantial + stricter vetting requirements

Meeting identity assurance requirements

- IAL2 is required for FISMA Moderate systems. RAF high can be an acceptable alternative. RAF v2 makes that easier.

- Increasing number of commercial providers of IAL2 identity proofing services are approved by the Kantara Initiative Assurance Program. They are listed at

  https://kantarainitiative.org/trust-status-list/

- InCommon members developed the *REFEDS Assurance Framework Implementation Guidance for InCommon Participants*

  http://doi.org/10.26869/ti.157.1

REFEDS MFA and assurance implementation by TLD

MFA	
be	1
ca	10
ch	6
com	1
cz	1
edu	186
fi	4
gov	3
my	1
nz	1
org	6
se	1
uk	4

ID Assurance	
be	1
br	2
ca	3
cn	1
com	1
de	42
edu	70
fi	8
gov	2
gr	1
in	3
org	2
pl	1
se	8
uk	1

Data gathered by

- successful NIH eRA login or
- successful NIH Compliance Check Tool test

June 21, 2021 - October 1, 2022

RAF adoption in DFN-AAI

- Broad willingness of Home Organisations to adopt and support the REFEDS Assurance Framework (although very few Service Providers require it yet)
- The reference frameworks are sometimes contradictory, too vague or outdated (i.e. difficult to find – Kantara SAC)
- Tendency to be overcautious and assert /IAP/low instead of /IAP/medium
- More courageous in terms of /IAP/local-enterprise
- Preview of RAF 2.0 very promising
    - Concrete examples and explanatory texts most welcome

Update from Wolfgang Pempe 30 November 2022