ASSURANCE IN ACTION

1- IMPLEMENTING ASSURANCE – YES WE CAN!

KYLE LEWIS
MATTHEW ECONOMOU

2 - EVOLUTION OF THE REFEDS ASSURANCE FRAMEWORK

JULE ZIEGLER

National Institute of Allergy and Infectious Diseases

Implementing Assurance…
Yes We Can!

Kyle Lewis (RDCT)
Matthew Economou (RDCT)
NIAID International Biomedical Support Team

7 Dec 2022

TechEX: Identity and Access Management

NIAID

Topical Agenda

Three links in Assurance "Chain of Custody"

- Establish: Identity Assurance
- Preserve: Authentication Assurance
- Communicate: Signal Assurances to Federation

…implemented over two frameworks:

- *(Establish and Communicate)*
  REFEDS Assurance Framework (RAF)
- *(Preserve and Communicate)*
  REFEDS MFA Profile

NIAD

Assurance Horizon

- Service Providers (SPs) drive adoption of assurance standards by requiring IdPs to implement and signal assurances
- NIH Requirements
  - MFA is here
  - Identity Assurance is coming
- REFEDS frameworks provides common glue make assurance in a federation possible
  - REFEDS Assurance Framework (RAF)
  - REFEDS MFA Profile

Our REFEDS Assurance Framework (RAF) Journey

- Two IdPs for ICERs in Africa: Mali and Uganda
- Each < 1000 users
- Complex environment: different levels of integration with host-nation IT at each site; multiple sponsors

- Goal: Implement RAF!

Implementing RAF at existing IdPs:

- New Users: do we need to adjust our process?
- Existing Users: what about existing accounts?
- And what even are the IAPs (Identity Assurance Profiles)?

ICER = International Center for Excellence in Research
IAP = Identity Assurance Profile

Starting Point: ‘Rules of Thumb’

(we required in-person proofing ... at some point along the way)

IAP LOW

See the user is a living person

IAP MEDIUM

+ visually inspect Govt Photo ID

IAP HIGH

+ check another trusted source

“authoritative to the context of the registrar”

National Institute of Allergy and Infectious Diseases

(We also created IAP “Zero” internally)
(‘Local Enterprise’ not our model)

NIAID

Two Key Points

- Transitive Property

- Not every user needs same IAP level
  - RAF is to be signaled per user, each login, not required to be same answer across all Institution

Example: ICER Uganda Implementation

- How does our current process work? Can we leverage existing HR hiring processes?
  - noted that HR process after a certain date was stronger than HR process before a certain date
  - 'chain of custody' of assurance achieved by HR's identity proofing procedures, and in-person HR handoff to IT desk for account creation
- All employees hired after a certain date: IAP-High
- All employees hired prior to that date: IAP-Medium.
  - (Can upgrade to HIGH if needed through HR reverification; Not all of these users need federated access).
- A certain number of users at remote site require only local access and were never ID proofed: remain at "IAP-Zero"
  (i.e., NO RAF Assurance signaled!)

So Now What?

We assigned users to various IAP levels… but we're not done:

Two questions remain:

- (1) How do I preserve assurance after this one-time identity proofing process?
- (2) What do I need to do in order to 'wire up' the tech to communicate identity assurance to federated SPs?

Preserving Assurance “Chain of Custody”

How sure are we that each login is the same person for whom the account was created?

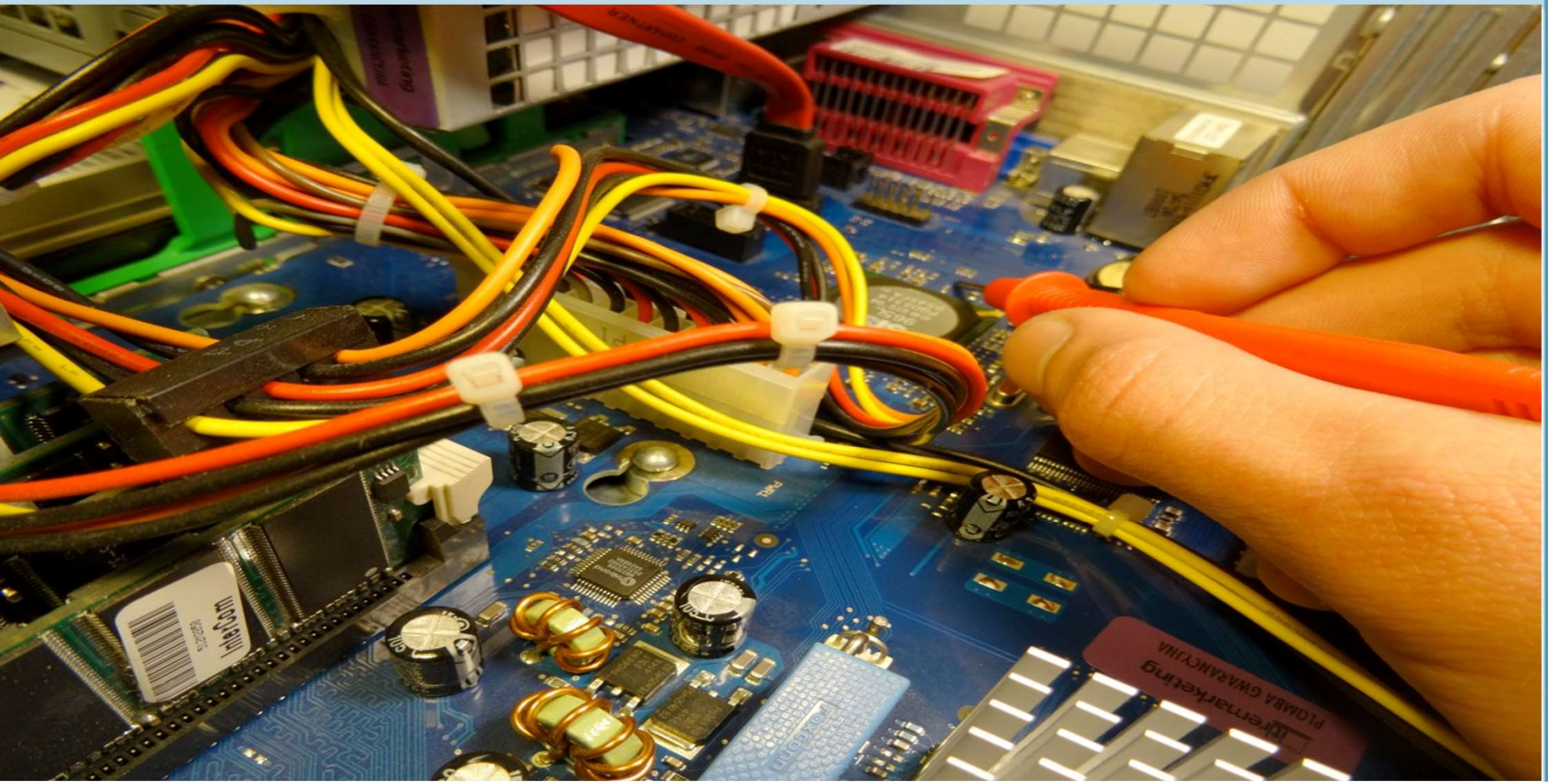
- Authenticators help preserve identity assurance through the life of the account
  - NIST IAL-2 requires AAL-2 (MFA*)
  - (same logic) REFEDS IAP-High needs MFA*
    (may be articulated through the REFEDS MFA Profile)

NIH National Institute of Allergy and Infectious Diseases

NIAID

*strong/effective MFA;
SMS texts not gonna cut it

Wiring It Up…



NIAID

Implementation Constraints

- Accounts synced between on-prem AD and Azure for Exchange 365 migration
- Users mostly have feature phones—
  no budget for hardware tokens or MFA as a service
- IT cannot support different MFA methods for Shibboleth and Azure

Key Insight: Use Azure, not AD

- Suggested by Chris Phillips at CANARIE
- Enforce MFA for mailbox access
  (a/k/a Microsoft “modern authentication”)
- Delegate federation authentication to Azure using Shibboleth IdP v4.0’s SAML proxying feature
- Simplifies user training, onboarding, and support

Recording Identity Assurance

- Assurance level stored in AD groups synced to Azure
- **IAP Zero** means unproofed, IdP-of-last-resort users
- Nested groups implement IAP level ordering (e.g., **IAP High** is a member of **IAP Medium**)

Name	Group type	Membership type	Source
EA eduPerson Assurance - IAP Zero	Security	Assigned	Windows Server AD
EA eduPerson Assurance - IAP High	Security	Assigned	Windows Server AD
EA eduPerson Assurance - IAP Low	Security	Assigned	Windows Server AD
EA eduPerson Assurance - IAP Medium	Security	Assigned	Windows Server AD

NIH National Institute of Allergy and Infectious Diseases

NIAID

Signaling Multi-factor Authentication

- MFA enforced by Azure but not signaled properly
- Overwrite Azure's authentication context with the REFEDS MFA profile

```
<util:map id="shibboleth.PrincipalProxyResponseMappings">
    <entry>
        <key>
            <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:Password" />
        </key>
        <list>
            <bean parent="shibboleth.SAML2AuthnContextClassRef"
                        c:classRef="https://refeds.org/profile/mfa" />
        </list>
    </entry>
</util:map>
```

Signaling IAP Levels

- Map group memberships to eduPersonAssurance values via ScriptedAttribute
- **DO NOT** give unproofed users **IAP Local Enterprise**

```
<AttributeDefinition id="eduPersonAssurance" xsi:type="ScriptedAttribute">
    <InputDataConnector ref="passthroughAttributes" attributeNames="azureGroups" />
    <Script>
        <![CDATA[
            if (typeof azureGroups != "undefined" && azureGroups != null) {
                if (!(azureGroups.getValues().contains("IAP-Zero"))) {
                    eduPersonAssurance.getValues().add("https://refeds.org/assurance/IAP/local-enterprise");
                }
                if (azureGroups.getValues().contains("IAP-Low")) {
                    eduPersonAssurance.getValues().add("https://refeds.org/assurance/IAP/low");
                }
```

Resources

Using SAML Proxying in the Shibboleth IdP to connect with Azure AD
https://shibboleth.atlassian.net/wiki/x/_YJxVw

Get NIH Ready
https://spaces.at.internet2.edu/x/goIgCw

CILogon Campus Identity Provider Test Page
https://cilogon.org/testidp/

Assurance in Action!

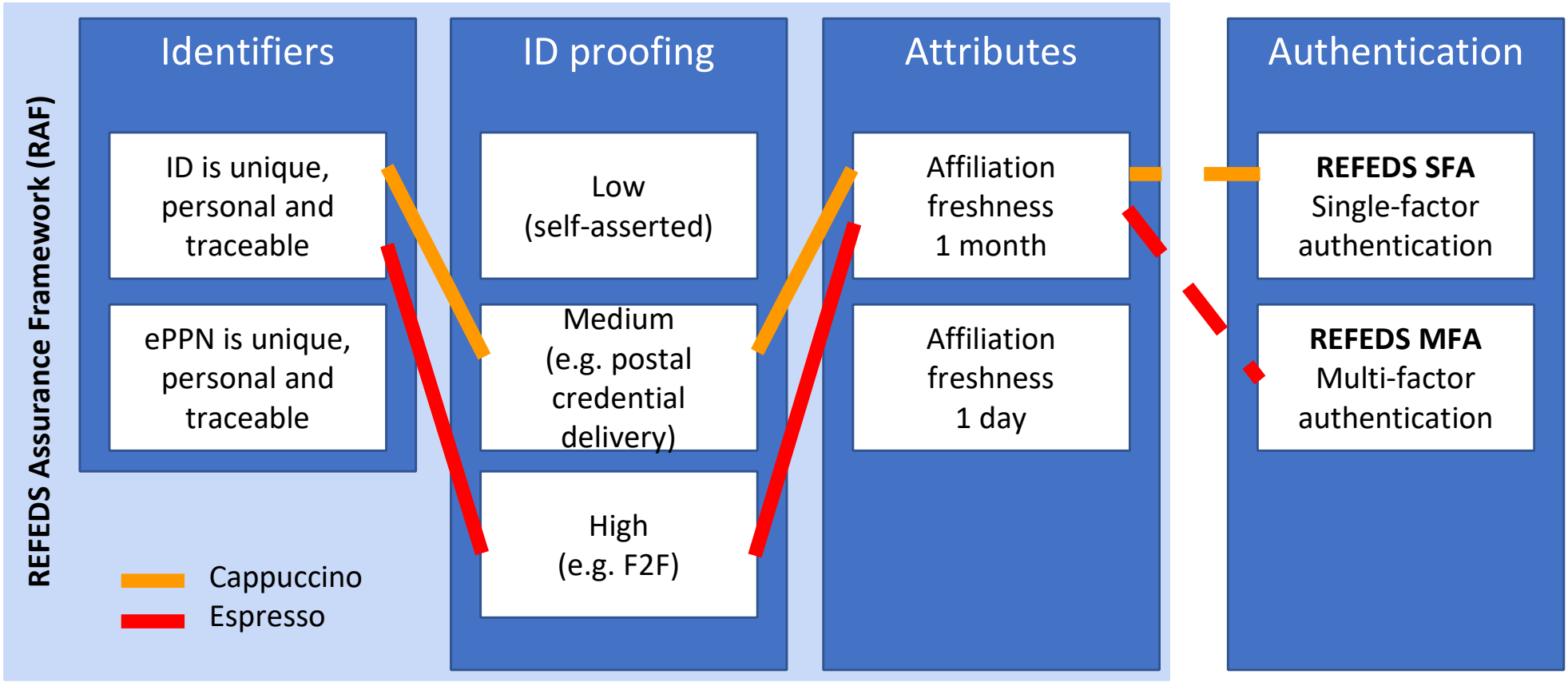
The Evolution of the REFEDS Assurance Framework

Internet2 Technology Exchange 2022, 7 December 2022
Jule Ziegler, LRZ/DFN, REFEDS Assurance WG Chair

REFEDS Assurance Framework (RAF)

- REFEDS Assurance Framework: https://refeds.org/assurance
- V1.0 Published (current)
- Defines a set of assurance tags for the eduPersonAssurance attribute in three different areas
  - Uniqueness of identifiers
  - Identity proofing
  - Affiliation attribute freshness
- Defines two combined assurance profiles
  - Cappuccino for moderate assurance
  - Espresso for high assurance

The big picture of assurance in REFEDS



RAF 2.0 Draft

- **Why?** Make REFEDS RAF easier to understand and use, both by IdPs and SPs. Remove any ambiguity, bring text to document
- **Who?** REFEDS Assurance WG, open forum, participation welcome
- **What next?** public consultation! (Probably after MFA profile consultation phase)

MFA Profile Consultation

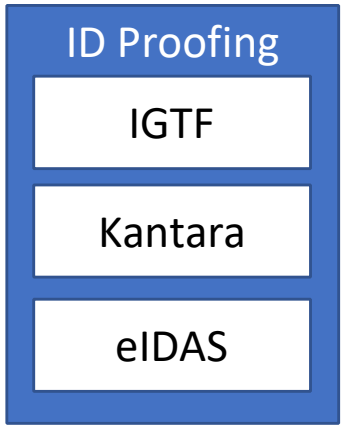
- Driven by requirements from the National Institute of Health (NIH) in 2021, which called for action
- Main Outputs of REFEDS MFA Subgroup (child of REFEDS Assurance WG) so far:
  - MFA Profile FAQ (informative)
  - MFA v1.1 (normative)
  - Editors' note for REFEDS MFA Profile v1.1
  - Public consultation until mid January 2023 - **please provide feedback!**

RAF 2.0 Draft - highlights

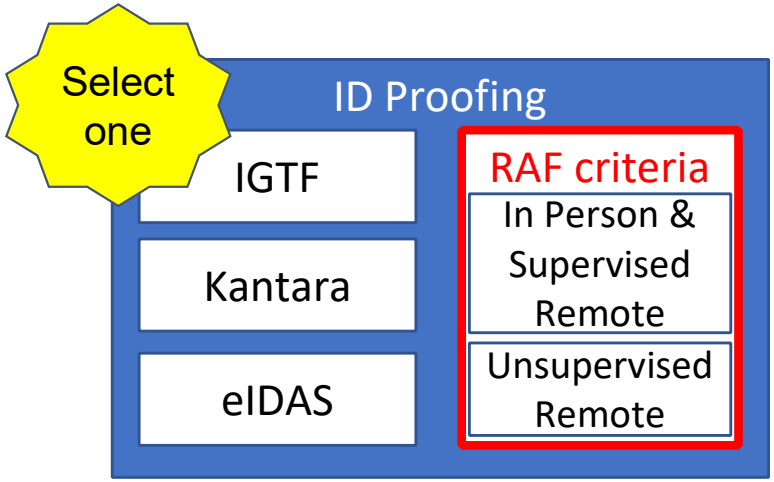
- 3 main areas (Identifiers, ID Proofing, Attribute Freshness) will be retained
- Updates on Identifier Uniqueness, such as usage of multiple identifiers
- **Major Update on ID Proofing section**
- make ‘local-enterprise’ more prominent in the spec
- text formatting including restructuring, glossary update, highlighting normative vs. informative text

ID Proofing Updates

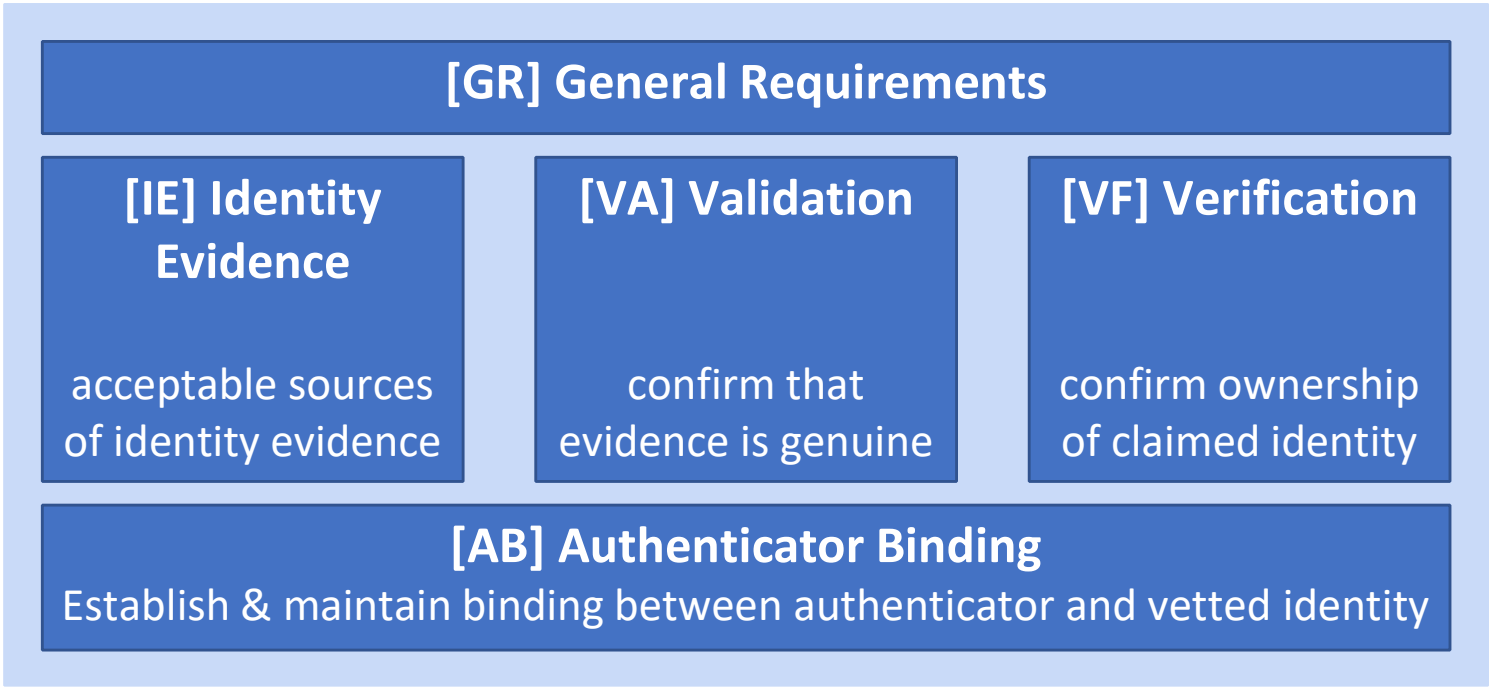
- ID Proofing part currently refers the reader to external standards



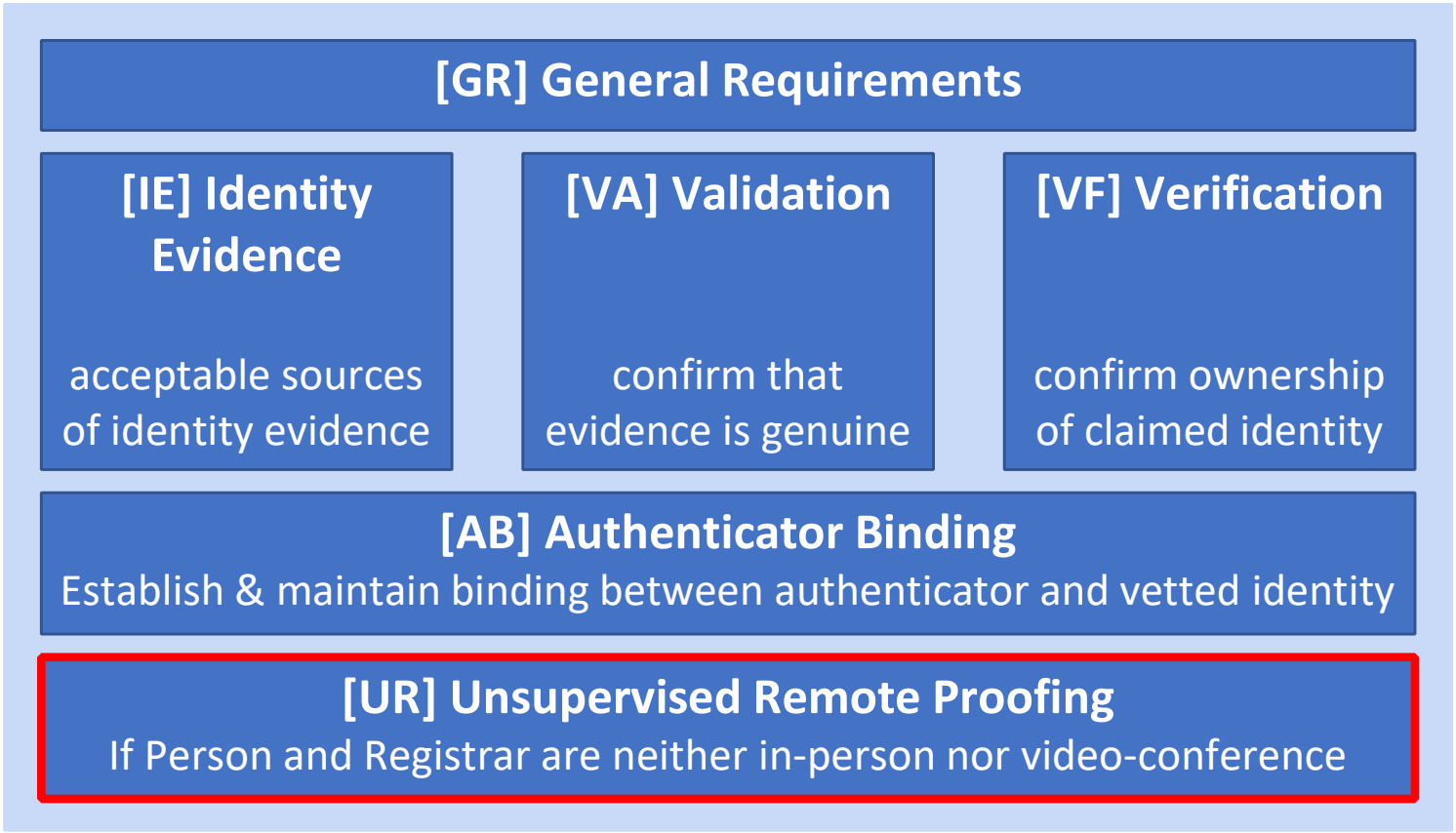
- RAF will now include its **own criteria** for each IAP level
- **new use case** (unsupervised remote) included



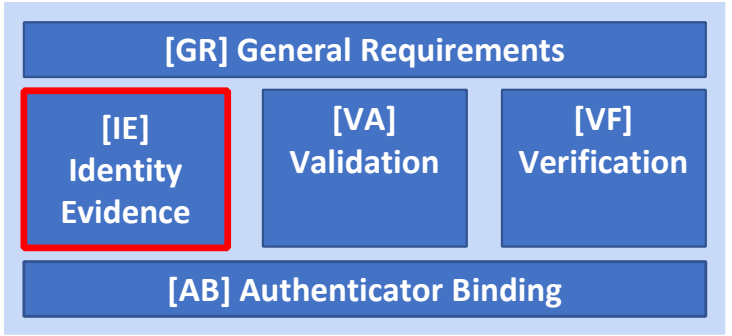
In Person & Supervised Remote Proofing

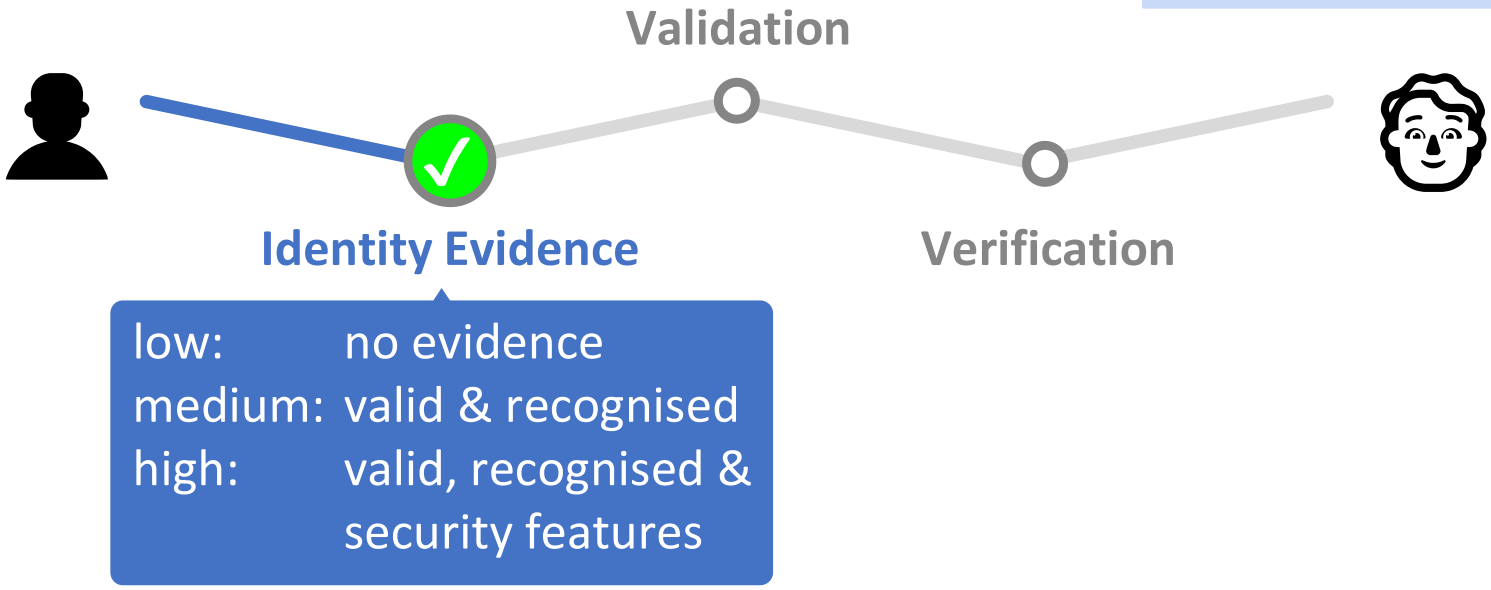


Unsupervised Remote Proofing (optional)



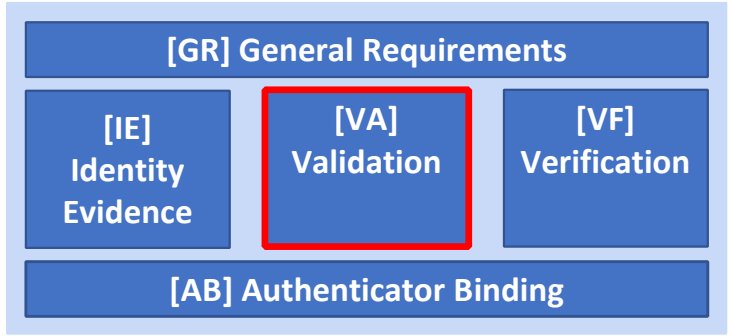
Identity Evidence, Validation & Verification

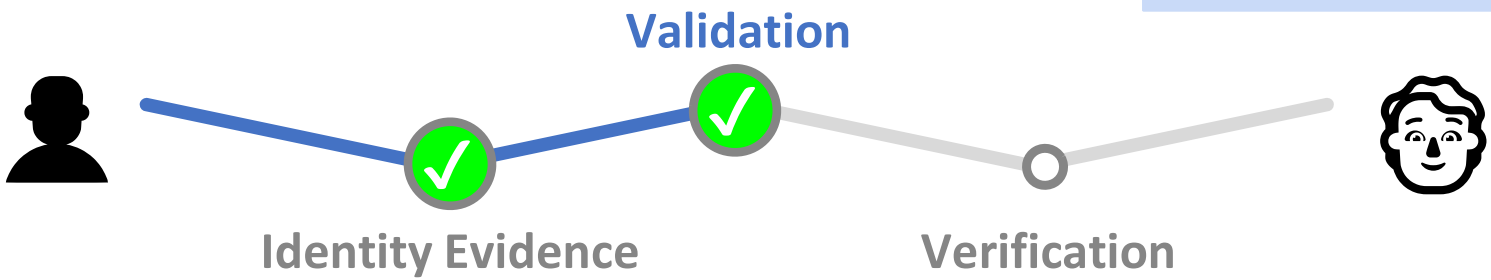




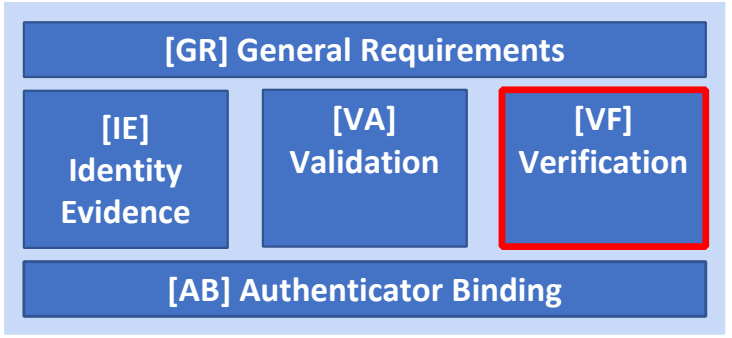
Identity Evidence, Validation & Verification

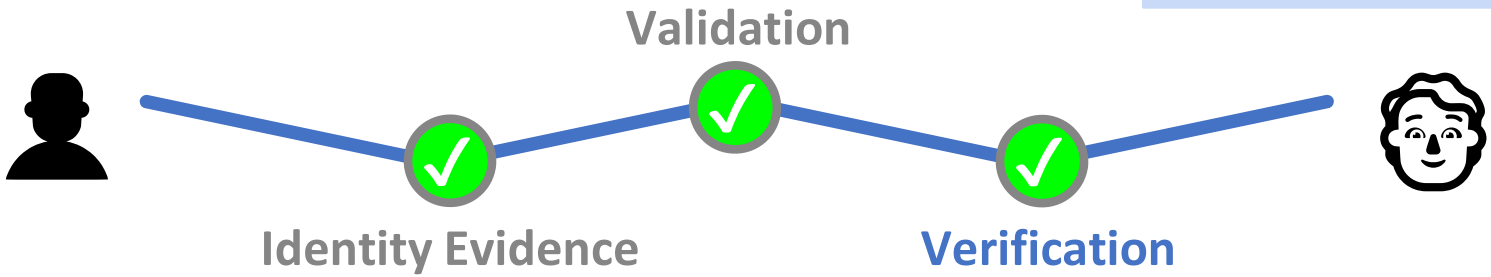
low: no evidence documents
medium: seems genuine
high: checked to be genuine & against trusted source





Identity Evidence, Validation & Verification

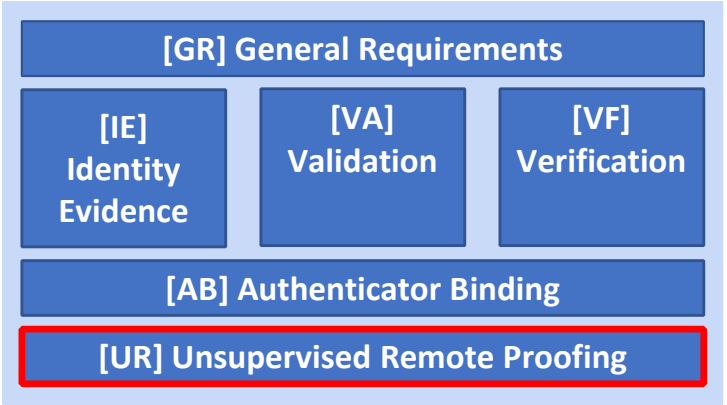




low:	Claimant is a Person
medium/ high:	Claimant is a Person & identity evidence reasonably belongs to Claimant

Unsupervised Remote Proofing

- e.g. fully automated proofing process
- Additional measures to accomplish IAP medium and high



BUT, only implement [UR] if you have such process in place!

→ I.e., [UR] is not required to claim one of the IAP levels

Good to know

- all requirements are reflected in a formal text & supporting table
- cross references between blocks possible, e.g:

  "*[UR2]: [VA3] is required.*" (text of suggested RAF change)

- IF-Statements included, e.g.:

  "***If*** *the CSP permits the Claimant to register a previously issued authenticator, then the Claimant must demonstrate control of that authenticator to the CSP during the identity proofing process."*

  (text of suggested RAF change)

Conclusion

- Work in Progress - but almost done!
- If you would like to contribute, visit:
  - REFEDS Assurance WG: https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group

Questions?