Assured Access Working Group Charter

Problem Statement

Some research service providers (SPs) and others face increasing need to demonstrate that their users have been well identity-proofed and that their authentication credentials are multifactor and well-bound to the user. These needs are incumbent on the users' Identity Providers (IdPs). This WG will identify and document processes that may be available at least to US academic organizations that can form the basis for asserting corresponding levels of assurance of identity proofing and credential binding.

How well identity-proofed and how well-bound the credentials will be is determined by reference to the IAP levels of low, moderate, high, and local-enterprise as defined in the REFEDS Assurance Framework (RAF). RAF itself aligns these values with well-known standards such as those developed by the Kantara Initiative. IGTF, and eIDAS.

The WG should aim to release an initial form of its guidance on an urgent basis to enable at least some academic institutions to address them before the NIH will require IAP Moderate, currently expected in June 2021. The WG may decide to continue work on a more comprehensive set of recommendations after its initial release.

Stakeholders/Influencers/Influences

- IAM architects at InCommon participants organizations
- Commercial and non-profit IdM providers, including Identity Management as a Service (IdMaaS) providers
- InCommon Federation (Internet2) management
- REFEDS Assurance WG
- Federated Identity Management for Research (FIM4R) community
- NIH CIT
- Research Data and Communications Technologies (RDCT), consultancy to NIAID that has studied these issues closely
- NERSC, ditto
- Kantara Initiative Assurance Program, which assesses Credential Service Providers and related component services and is accepted by the US Government for validating adherence to NIST 800-63-2 and 800-63-3. The WG may consider asking their opinions of draft guidance.

Charter

The AA WG will:

1. Solicit input from InCommon Participants and other parties who have related experience to try to identify a set of approaches to dig further into.
2. Determine guidance for use of the I9 process in assigning IAP levels for the WG's initial release. In particular, consider the role of e-Verify for employers enrolled in it.
3. Assess the potential role of referral processes as compensating controls for some identity proofing steps. Egs:
    a. A Principal Investigator whose identity has been sufficiently proofed confirms identity evidence submitted by their collaborator.
    b. An instructor or advisor whose identity has been sufficiently proofed confirms identity evidence submitted by their student.
4. Determine guidance, supplemental to criteria defined in NIST 800-63, Kantara, and related standards, on ways that credential issuance, renewal, and replacement can be linked to a vetted identity, including
    a. In person, such as ID Card issuing or HR processes
    b. In association with commercial services that validate identity evidence, eg, via an API.
    c. Compensating controls, ie, ways that a credential can be reasonably inferred to be controlled by the proofed identity it was assigned to. Example: if a credential is required to route employee paychecks to their bank, can it be inferred to be well-bound to that employee even if the credential issuance process does not itself accomplish the linkage?
5. Proceed as quickly as possible. Consider meeting weekly rather than the typical biweekly cadence. Consider assigning some tasks to subgroups to work in parallel, bringing final drafts to the full WG for review.
6. Share information and coordinate with the REFEDS Assurance WG.
7. Recommend other working groups that may be needed, eg, to address similar needs in other countries.

Out of Scope:

1. Develop guidance for how to use the REFEDS MFA Profile in certain circumstances, for example, when the SP desires but need not require MFA, or when an IdP's MFA system is temporarily unavailable. The REFEDS Assurance WG is taking this up - interested parties should participate there.
2. Align NIST SP800-63A with RAF IAPs. The REFEDS Assurance WG is taking this up. However, the AA WG may decide to reference 800-63A or 800-63B in its guidelines.
3. Outreach activities to deliver the WG's guidance to InCommon Participants and related support activities. These will be undertaken by InCommon.

Membership

Membership in the Assured Access Working Group is open to all interested parties. Solicitation will take place on lists such as the InCommon Participants list and the REFEDS list, explicitly seeking international participation. Some stakeholders may be explicitly solicited by the Co-Chairs or other Working Group members for participation, e.g., providers who do not ordinarily participate on the above lists. Members join the Working Group by subscribing to the mailing list and Slack channel, participating on the calls, and otherwise actively engaging in the work of the group.

Work Products

1. An initial form of guidance, to be issued as soon as possible. Perhaps focused on the I9 process.
2. Additional guidance to institutions on processes available for indicating assurance.

Appendices and Resources

- NIH Compliance login test: https://authdev.nih.gov/CertAuthV3/forms/compliancecheck.aspx
- electronic Research Administration (eRA) Commons: https://era.nih.gov/
- Form-I9 Training and Webinars: https://www.uscis.gov/i-9-central/form-i-9-resources/form-i-9-training
- REFEDS Assurance Framework: https://refeds.org/assurance

See Also

* Original draft charter in Google Doc