Validating users from non-qualified IdPs

Scope and applicability

This process is applicable to information services where the impact of breaching the security objectives (confidentiality, integrity, availability) is **limited**, and the guidance here should not be applied as-is to services whose information categorization (in terms of e.g. FIPS199) is moderate or high. In a federated context, where trust needs to be transient, it should be interpreted such that the risk to the service provider itself is limited, and the risk to other federation members does not materially increase - within the context of the federation agreements - as a result of this process.

For GOCDB, when the available per-resource provider and per-user role model is applied, the most significant risk is that of breached confidentiality, in particular that of communications sent to site administrators and security contacts listed in GOCDB that are used by consumers to send restricted (confidential) information and notices.

Given the need to identify users and assign them persistently to communities, groups, and GOCDB "sites", vetting should materially meet the R&S and Sirtfi requirements. This includes meeting at least **https://refeds.org/assurance/ID/unique** and **https://refeds.org/assurance/IAP/low**, and in addition requires a (non-opaque and not-intentionally-confusing) person name.

IdP requirements

The IdP must either implement all relevant controls itself, or leverage an external (social) ID source capable of meeting ID/unique and IAP/low requirements and augment that information in accordance with AARC-G041 [1]:

> The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through heuristic or other business logic, that provide additional keys to 'who they are' and that the user is a single natural person and not sharing the account. **The social ID(identifier) itself is never re-assigned**.
>
> In addition either the Proxy or an 'upstream' identity source provides a valid email address through which the user can reasonably be expected to be reached

In order to materially meet Sirtfi requirements, the IdP should be operated according to current good IT security practices, indication of which may be obtained from its Privacy Policy and Terms of Service. Such documents must be available, compliant with statutory and regulatory requirements, and be sufficient to have the ability to implement Sirtfi requirements.

The following IdPs are known to meet the above:

- EGI SSO provider
- Google (identity provider services)

User requirements

The unique identifier (SAML subject-id attribute, OIDC sub claim, IGTF Subject DN) must be associated with a verified email address and a reasonable representation of the user's real name to the extent provided by R&S plus Sirtfi.

If an account from a non-R&S IdP can be linked to an existing account, the combination of assurance information in accordance with AARC-G031 [2] may be used to meet the requirements. If an R&S-Sirtfi account can be associated, the account must be persistently linked and no further steps need to be taken.

Otherwise, correctness of the R&S attributes must be confirmed before or during COU enrolment by a registration agent (RA), trained and appropriately authorized by the COU authority. The COU system in addition must implement the user-facing aspects of the Sirtfi requirements (traceability and user management capabilities).

Following this process makes these accounts materially equivalent to R&S + Sirtfi.

Prerequisites

The RA and the applicant must have a pre-existing business relationship, and the application must take place in context.

The applicant must provide

- the unique identifier or verified email address as will be obtained from the IdP
- email address, as conveyed via the authentication action
- Full name
- Organisation name (e.g. institute name)
- Application context, i.e., description of existing business relationship

The applicant should provide

- secondary, institutional, email address for account recovery purposes

Verifying email

If the domain name part of the email address is registered to and owned by the IdP operator, and the email address is asserted as part of the act of authentication, no further confirmation is required.

For other email addresses, the control over the mailbox must be established and linked to the application by means of a nonce-challenge-response method.

Verifying organisational affiliation

Use of a organisation email addres, or a check by the RA that the verified address address is listed in a trusted information source representing the organisation (such as the organisational web site) sufficiently confirms affiliation.

In absense of this, the RA calling the user via the main (exchange) phone number of the organisation as obtained from a trusted information source and verifying a challenge sent by email to the address is sufficient.

Verifying applicant full name

The name can be asserted to by the RA is the agent has had prior in-person meetings with the applicant, and the application is verified by a call or text message to a number on the existing address-of-record.

The name can be asserted in a video-supported tele-meeting in which the applicant meets with the RA, during which the photo-ID document is presented and verified for authenticity.

> For a tele-meeting, relevant compensatory controls should be put in place. For example implementing a process where:
>
> - the RA must initiate the tele-meeting, and the tele-meeting shall have at least a resolution and quality sufficient to verify the authenticity details of documents and read documents shown in front of the camera, and be over secure channels when traversing the public internet,
> - the RA shall only authenticate documents of which the RA is familiar with their physical form and authenticity properties, and verify such properties, including holographic and transparency elements,
> - unless deemed infeasible by the RA, the applicant shall demonstrate authenticity of photo-ID documents by showing – on video during the meeting - their real-time read-out via NFC, e.g. using the ReadID app, and show the serial number thus read-out to the RA over video,
> - the RA shall, to the extent possible, confirm the liveness of the applicant and the likeness with the image on the presented photo-ID.
>
> Sending a nonce (unique number) by email during the meeting may augment assurance in case of doubt.

The identify of the applicant may also be verified by the RA during an in-person meeting in which a photo-ID is presented and the name verified.

Implementing controls

The COU system must implement

- user suspension and termination without removing traceability information
- enforce AUP presentation and acceptance for the user

---

1. AARC-G041, Expression of REFEDS RAF assurance components for identities derived from social media accounts, **https://aarc-community.org/guidelines/aarc-g041/** , published March 2018. ↩

2. AARC-G031 Guidelines for the evaluation and combination of the assurance of external identities, **https://aarc-project.eu/guidelines/aarc-g031/** , published July 2018. ↩