INDIGO IAM Hackathon - Community Notes

Issues discussed are tagged in Github: [Issues · indigo-iam/iam]

Wednesday

IAM Development Update

+1 for configurable token saving from STFC, we can resume our geo-distributed HA work as this should improve the stability of DB in distributed settings.
Also, since this improvement is focused on write should be a more significant improvement since galera is write locked.

From STFC we prefer to have a more flexible MFA implementation, If possible a flexible endpoint that we can attach to IAM, so that it can be upgraded in a modular way.
Francesco: for the INFN IdP they use https://www.privacyidea.org/. Would this be an option?

STFC IAM Operations

High usage of STDC IAM instances - approx 900 for IRIS and 250 for SKA

Topic Requests

Request for an elevated role ("~VO Admin") user to be implemented who could approve people to join without requiring to be an administrator of the INDIGO IAM instance (with right to change groups, clients, delete users…). (If the initial user has to be set up by the global admin that's OK, but that user should be able to create more admins.) This would be needed as there is often zero overlap between these groups (VO admin/machine admin). Bonus points for at least limited debugging access for VO admin. Interested: Daniela (for XLZD), Michel (France)

We could open an issue about adding a new ROLE_VALIDATOR (name can be discussed). The capabilities expected for this role are:
- Accepting/Refusing registration requests
- Resending confirmation email

Discussion Sessions

MFA implementation discussion

Plug in module vs inbuilt function. Expectation for metadata around MFA to be released, but not always there, resulting in duplicate MFA.
Passkey implementation: Passkey is considered by some as a better implementation compared to TOTP, given the known issue for our TOTP implementation right now (library issue etc.), is it time to look at more advanced after the basic TOTP is done. Interested: STFC, JISC, Imperial.
OIDC is awkward when requesting ACRs

Support from JISC: OpenSAML plugin support

EOSC requirements - Missing scopes/claims

According to EOSC AAI Architecture 2025 document (https://zenodo.org/records/15388270), some of the required claims don't exist on INDIGO IAM aarc profile:

- name, given_name, family_name, email -> needs to be on introspection (already exist in others) VERIFIED
- schac_home_organization -> needs to be on userinfo, introspection VERIFIED
- voperson_external_affiliation -> needs to be on userinfo, introspection (there is already eduperson_scoped_affiliation, maybe can be reused?)
- Sub claim needs to be equal to voperson_id claim and needs to be scoped just like voperson_id
    - this isn't backwards compatible as the sub would change but this is needed for following the AARC guideline
    - Enrico: we can add a regex when we evaluate the sub of a token excluding the part following the '@'
    - Francesco: assuming the voperson_id is <sub>@<iam hostname>, isn't it enough to check that if there is an @ part, it corresponds to the iam hostname?

REGISTRATION REQUEST TIMEOUT
We could add a timeout in order to avoid users stuck on a not received confirmation email (because of a failure or a wrong email address). After a certain amount of hours (configurable) the request can be automatically canceled

- Maarten (Feb 23): by default the requests should stay in the queue (has served us well)

CONFIRMATION EMAIL

An IAM Authorization Failure event is logged each time the "/" path is requested. The request is correctly forwarded to /login but this logged message is really annoying and should be removed.
https://github.com/indigo-iam/iam/issues/1127

Implement account lockout after a configurable number of failed login attempts
https://github.com/indigo-iam/iam/issues/1133
We agreed that:

- We need to track the number of attempts and the last failure timestamp
- We can store these info inside another table related to IamAccount one
- A configurable delay is applied to the last failure timestamp if a configurable amount of attempts has been reached. During this delay, the user cannot login again.
    - If the configurable delay has been reached then we consider that as a 1 cycle. We can also configure how many cycles the user is allowed to perform the login attempts and then disable the user if the configurable cycle has been reached.
- We don't need to track the attempts done during the suspension delay (maybe not logging them too)
- These columns can be reused in case of failed TOTp codes.
- Implement a mechanism to enter totp after some delay.

eduGAIN SAML metadata refresh starts by failing at each refresh interval · Issue #884 · indigo-iam/iam

Discussed the cause of the metadata SSL handshake issue
Donald: https://github.com/spring-attic/spring-security-saml/issues/233 Probably the unexpected behavior described here about opensaml library. STFC/UKfed use only http endpoint.