SESSION #4, Breakout #4

Session Title: Deprovisioning from IdP, community proxy and services
Session Convener: Andreas Klotz
Session Notes Taker(s): Floris

Tags / links to resources / technology discussed, related to this session:

-
- OpenID Provider Commands 1.0 - relevant for deprovisioning?: https://github.com/openid/openid-provider-commands
- https://openid.net/specs/openid-provider-commands-1_0.html

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion, action items, next steps:

Service: a federated way to log in to a service, and then the service provides the option to create a local account. Deprovisioning will not work.

The SSH scenario is different:

Storage has a different deprovisioning issue: once a user stops logging in, what to do with the storage?
That is more a Research Data Management issue, then a deprovisioning issue.

- Data protection, right of being forgotten
- Data preservation

There might be ways of accessing data without logging in (visibly for the IdP and proxy).

There might be communication from the IdP to the proxy, or from the proxy to the users about inactivity or expiring identities or permissions.

The hard part about account linking is account unlinking, which is similar to deprovisioning. For example, a user used their university ID to log in and create an SSH key. After the user is no longer with the university, the SSH key persists.

Don't expect (home) IdPs to play any active role in deprovisioning.
So we need to look to the proxy for solutions.

A problem with a proxy telling the service when a user was last active, is that proxies implement this in different ways.

So we might make an AARC standard of deprovisioning: possibly OP commands, or SCIM.

OP commands is focussed on getting account status. SCIM is also about keeping information in sync.
In the OP commands draft spec, the OP sends info to the RP, so the RP needs to implement an endpoint. SCIM can be both pull or push.

Indigo IAM, Unity IDM, and Keycloak have SCIM interfaces (Keycloak through an extension).

So, we need some architecture discussion about a new guideline about deprovisioning?
Well, there might be nothing to do?
We are going to use SCIM or OP commands, but we might want to define a SCIM schema for deprovisioning and/or a last active timestamp for the user.