Yoda user provisioning -> SRAM

a service provider perspective

Agenda

- **Current situation: Local identities**
- **Target situation: Federated identities**
- **Analysis: Collaborations and SRAM**
- **Provisioning Yoda users to SRAM?**

Current: Services use local identity

- **Local organization taken as Center of the Universe**
  - Users access local services via institutional ‘home’ account
  - Third-party users are provisioned with “Guest” account
- **Third-party access is flawed**
  - To limit (license) cost, guest accounts are limited
  - To limit security risks, guest accounts not fully authorized
- **It is a hassle for users**
  - Need a separate account with each organization/service

Current: ‘local’ identity insufficient

- **External user access to local services is informal**
  - Access granted to guest where a local user acts as sponsor
- **Advantage:**
  - Works well for small, informal collaborations
- **Disadvantage:**
  - Local user becomes liable for actions guest user
  - Policies not enforced

Target: Federated identity

- **Similar logon for local and external users**
  - e.g. SURFConext as federated identity authentication service
- **Advantages:**
  - User-friendly: User can use home account credentials for authentication across services
  - Policy: Improved identity assurance external users
  - Policy: formal acceptance of service access by external org.
- **Disadvantage:**
  - Each external user organization needs to opt-in for service

Consortium needs beyond Federation

- **The consortium is responsible for data processing**
  - (Not the institutes, but) the consortium signs processing agreement with a service
  - The coordinating organization of the consortium usually represents all partner organizations (that remain liable ultimately)
- **Service access determined by consortium membership**
  - Authorization is based on consortium membership, not on an institute affiliation

NB: The SRAM implementation of consortium concept is “collaboration”

SRAM supplements SURFConext

- **SRAM maintains collaboration memberships and -services**
  - Unified view on collaboration member identities
  - Collaboration signs opt-in to service for members
    - Suitable for authorization of services that grant access based solely on collaboration membership
- **SURFConext unifies view on affiliated identities**
  - Asserts that authenticated user is affiliated with an organization (can be returned as attribute)
  - When used in SRAM context: user (still) represents the partner organization as a member

SRAM implications for services

- **Authentication:**
  - Services must make a de-provision workflow for user identities, since SRAM identity will expire after CO membership ends (and data might be linked to the identity)
  - Service may need to integrate with alternative authentication methods to support access for identities that are not member of an SRAM registered CO.
- **Authorization:**
  - The service must (be adapted to) support *multiple* tenants, as CO membership maps to “authorization to data per CO”.

Example: SRAM projected to Yoda

- **Option A:**
  - SRAM CO → Yoda Category
  - SRAM CO-Group → Yoda Research Group + Role
  - Disadvantage: separate Yoda Groups needed per Role
- **Option B:**
  - SRAM CO → Yoda Research Group
  - SRAM CO-Group → Yoda Research Group role
  - Disadvantage: mapping of policies (Category) missing

Autoprovisioning Yoda users->SRAM?

Assumption: SRAM replaces Yoda external user service

- **New insights:**
  - Not sufficient to map users, need to map CO as well
  - Need for processing agreements between CO and Yoda
  - SRAM API under revision: provisioning not yet feasible
  - SRAM makes it easier for a CO to use a service (opt-in)
- **Conclusion:**
  - Access to Yoda for SRAM identities (SSO) can be pursued
  - Too early to consider provisioning strategies SRAM/Yoda