(A Few) Identity and Access Management Workflow Requirements

RL “Bob” Morgan
University of Washington
ACAMP Workflow, Burlington, VT, June 2006
Many identity and access management (IAM) processes are classic administrative operations that would benefit from workflow-enablement.

Workflow process definition and privilege management share many features.

This talk considers these requirements.
MACE IAM Model

Systems of Record

Join

PROVIDE

Provision

Registry

Privilege

Person

Group

Mware Systems

Mware Services

AuthN

WebSSO

PROVIDE

Relay

AuthZ

Log

Apps

Systems of Record

Manage Cred's

Manage Priv's

Reflect

SIS

HR

Alums

Admissions
Person registry

• key operation is person matching
  • determine whether two records are one person, based on matching data, at record input time, or via scheduled processing
  • often judgment call, i.e. requires approval
  • match resolution triggers further processing

• person/account sponsorship
  • workflow for approval, id establishment
Many services provided to an individual are based on affiliation status and other inputs, with service changes triggered by transitions.

Often thought of as FSM:
- User/manager notifications part of process, e.g.

Can be modeled as workflow process? aka business process?
Provisioning

- Driving accounts/settings in managed systems from central data
- Support incorporation of sysadmin/manager action in process flow?
- model target systems acceptance processes as workflow?
Privilege management

- simple priv: subject A can do op Y on res Z
- workflow-based priv:
  subject A can do Y with approval of B
- approval as priv:
  subject A can approve action X
- workflow in priv management delegation:
  subject A has authority for X, but must be approved by B
Federation policy management

- Shibboleth attribute release policy
  - what user attributes go to which consumers
  - in-band user approval step as workflow?
  - group policy management needs workflow?
- adding new federated participant
  - to federation as a whole
  - to site's business partner list: evaluation of site policies and procedures, etc
Virtual organization support

• VO

• is activity involving participants and resources from many real organizations

• needs collaboration infrastructure, preferably supported by one or more ROs

• workflow services as VO support component? Implies interoperable workflow among VO participants, resources?
Workflow and event flow

- IAM middleware often integrated via event/message bus
- does workflow have well-defined relationship to event/message architectures?