“FIM: Land of Open Issues”

Peter Schober, ACOnet

TTC, July 8, 2015

Topics

Somewhat arbitrarily chosen starting points, all interrelated:

- Authentication
- Authorisation
- Provisioning
- Attributes
- SSO

- Issues I'm currently dealing with

Authentication

- Passwords, yawn!
- Phishing, still...
- Strong authn, 2FA, MFA
  - Related to Vetting, Assurance
  - Standards, software & protocols (RPs may want to know)
- Password reset procedures/tech
  - See above (vetting, assurance)

Authorisation

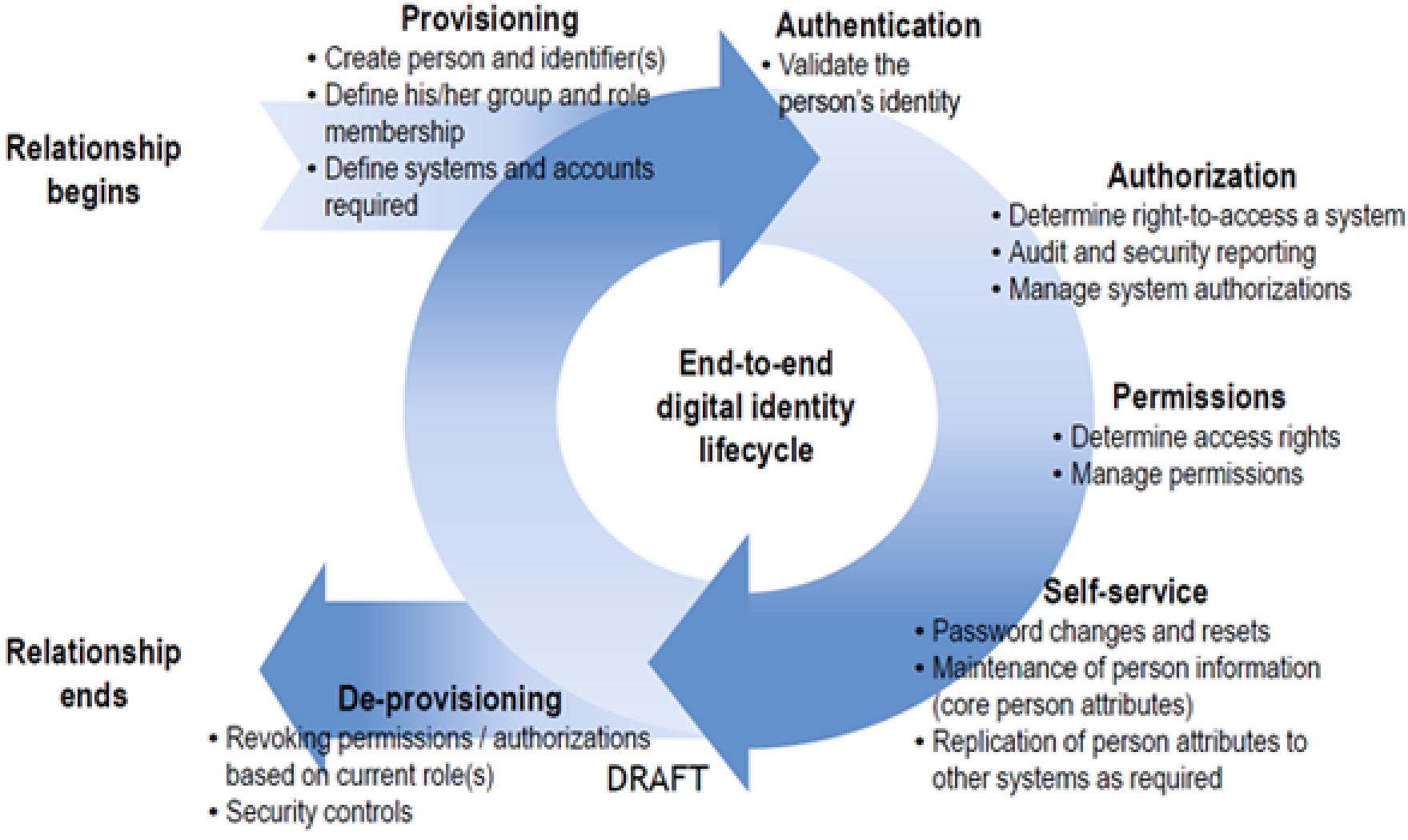
- Fine-grained (calculate/mint/provision) vs. coarse (available)
- "What I have" (entitlement X) vs. "What I am" (affiliaton "staff")
- Work for IDP (pre-calculate Joe's rights for SP X) vs. SP
- Seperation of duty (authN / authR), some don't do their part:
  - Library SPs: "We dont need any attrs" ≠ their license terms
  - GAFE/GAFYD (won't do authR and/or charge per user)
  - Pushes authR into the authN process, ever more complex
    - (context-dependent MFA, Consent, pre-authR per service, …)
- Data req for authR may be unavailable ("academic", tcs-user)
  - or unsuitable (birthdate vs. "of legal age")

Provisioning

- "Just-in-Case" (JIC, e.g. batch) vs. "Just-in-Time" (JIT, e.g. SSO)
  - JIC has Issues with Federation
  - JIT has issues with authR
- Apps operate on local accounts, e.g. Confluence
  - JIT account creation w/ SSO works fine, but
  - assigning rights/permissions reqs local acc to exist!
- Deprovisioning
  - Hardly works within an enterprise
  - Make apps keep track of "TTL" and cleanup stale data/ACLs
- Guest accounts: Who's responsible? Expiration? What attrs?

  authn vs authR

Identity Lifecycle model, ubc.ca



Attributes

- Agreeing on data structures & on-the-wire representation
- Humans and their names (WP: naming customs, IBM wp)
- Identifiers & their properties, e.g.
  - persistent, revocable, reassignable, opaque, targeted, global
- Cost of supporting some of them (properly)
  - Stable IDs req'd, namespace depletion vs support nightmare
- Who gets what attrs (what data to send where)
- **Data protection, compliance, risk management**
- Who decides (institution, subject), based on what
  - "manual" admin processes, CIO, Entity Categories, Consent
- risk-based approach (R&S) vs. full compliance (CoCo)

Single Sign-On

- Application integration
  - Silo/Center of Universe → externalise authN, authR, sessions, …
  - https://wiki.surfnet.nl/display/domestication/
- “Integrated authN” (SSO from desktop, SPNEGO, Moonshot)
- Logout (“right-sizing” the issue, security vs. liability/blame)

Issues I'm currently dealing with

- Interfederation within .at
  - Interop with Fed for government administration (now w/ SAML)
  - Access to resources in the Austrian Federal Computing Centre
    - Hosted SAP ("One SAP to rule them all")
    - ID data for all pupils of federatal schools
    - Central citizen registry
  - Federal schools to get 1 central IDP + federate w/ SPs
- GEANT (Project) work
  - SA5T4 FaaS (moniker causes misunderstanding; not F-**OP**-aaS)
    - Best of breed tools, Registry + Aggregation + HSM
  - SA5T1 FedHarm (needs a better short title :))
    - e.g. Entity Categories: Library/affiliation services