Link to 2024 ACAMP Wiki

Advance CAMP Thu. Dec 12 2024

Room - III

Session Title: Identity First

CONVENER: Kevin Rooney (Virginia Tech)

MAIN SCRIBE(S): Julian Anderson (Oberlin College)

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 24

DISCUSSION:

- Kevin: we've been working with a Banner instance for 30+ years and trust that identities are merged, etc. before they come to us. That being said, Ellucian is forcing Banner customers to go to the cloud
    - We've been running PL-SQL extensions for years; in difficult position of not being able to run these in cloud
    - Now have two ERPs to work with -- how to do identity matching
    - We know we need to refactor everything
    - We already have Grouper in place; have had it for 2-3 years, it's fantastic, we love it. Does application policy mgmt
    - Putting midPoint into prod end of this month/early January, but will only be provisioning AD security groups in 1st iteration
    - We want to put midPoint at the center — identity first. We don't want *any* identities to be created unless data comes in from the ERPs and gets matched in midPoint

    - We at VT currently take the SPRIDEN ID from Banner. Ellucian says we'll take your SPRIDEN IDs now on-prem, but in cloud, can theoretically be provisioned centrally
    - Also, how do we pressure Ellucian to do what we want?
        - We have strong development power, but we also need Ellucian to play ball
    - Thoughts?
- Gabor Eszes (University of Virginia): walk me thru your process
    - Kevin: student applicant for roadmap purposes (only one going into cloud rn)
    - Gabor: we get basic demographic/identity data starting in CommonApp, fed to Slate
    - Kevin: Several PoCs in play: one is where we take a Slate payload of applicants, drop into AWS S3 bucket, have midPoint pull it and match it against metadata registry via LDAP, then insert person record into Banner via person manager API. We'd prefer to shove Slate identifier in there and stress importance of matching with it. Match what we can; pull out those that need extra work and put into extra bucket, which is then feed directly to Banner person manager. At that point, take all the identity data and update our identity systems w/ addresses, etc., push it out for provisioning
    - Gabor: for, e.g., employees: how are you getting them into midPoint?
        - Kevin: yep, this is a bear for us; for existing entries in HR on-prem system, they'll have an entry in the person registry. If they're a faculty member, midPoint will know that and provision to SaaS product with same SPRIDEN ID
    - Michael McNulty (Tufts): What is the problem we're trying to solve?
        - Kevin: We want to re-architect! Trying to turn things around from Banner as source of truth for provisioning, to central matcher & person registry
        - Michael: we have the same problem, but have deferred for political reasons. Challenges: it's a nightmare, esp as you deal w/ applicants. HR: as long as it does not interrupt (employee) application process
        - Michael: we did a PoC with Cirrus's Gateway product; grab identity info as Slate account is created
    - Gray Hudgens (University of Florida): Are you doing anything w/ account linking in Cirrus?
        - Yes. (e.g., person who signs up with Google once, Yahoo next gets matched to same NetID)

        - Per Gray, they've used that and it's worked well
    - Michael: Tufts does not yet have single unified university profile (e.g., disparate identities for undergrads, clinical folks, alums, etc., and a name change [for example] means different offices to work with for each identity type); hoping to push idea of central identity home whose updates are then pushed out to the various systems
    - Kevin: selling this to senior leaders is hard!
    - Julian Anderson (Oberlin): how did you get to using Grouper and midPoint w/ Banner?
        - Kevin: we had an administrative push for IGA backing us
        - Also, set math is hard. You can maybe get it going with your own system, but Grouper is *great* at set math!
        - VT has advantage of large IAM team (22) vs smaller schools (e.g., Oberlin has 3ish)
    - Colin McCarthy, UWash: 20-some identity sources, 6 of which are HR
        - We're so far from identity-first; we have to go to 30 plus stakeholders and make them work with us
        - Have to deal with response of "it works right now!" Well yes, because we can pretend certain ways of matching are practicable
    - Kevin: Ellucian VP of Identity claimed they were getting out of identity business, but they were going to integrate w/ Okta, Entra ID, maybe 1 more commercial product. Claimed no plans to work with InCommon TAP — maybe this needs to be a wake-up call for them that Internet2 schools are not going to be choosing their product!
    - Andrew Parmer (University of Wisconsin): Unfortunately, it's going to get harder.
        - Main type of IAM we see in higher ed is registry style and centralized (identity first) style. I have worked at schools that do both, but downside of centralized is that because you need that much more control, you need much tighter integration w/ identity sources. As part of increase of SaaS systems, inability to tie in as much as is needed to maintain centralized style/less willingness of vendors to deal with schools' boutique IDM processes?
        - https://profisee.com/blog/master-data-management-implementation-styles/
        - Scott Weyandt (Moran): is there a requirement that these all be unified into same identifier? Many clients of Moran have increasing situations

where non-traditional identities are increasing (e.g., community members, folks from other institutions taking a course). Value of central identifier might be decreasing over time, and some examples of clients (e.g., The Claremont Colleges) where there are multiple valid person identifiers in addition to a central ID

- Some institutions have multiple Banners so that SPRIDENs don't agree; highly recommend picking centralized, opaque identifier that is persistent regardless of ERP
    - Kevin: great that shadow identifiers exist and that's how a lot of IGA systems work, but we do have a particular type of identifier that gets put a lot of places (e.g., ID cards) that we need to be able to control and assert centrally

- Gabor: what is your fear here?
    - Andrew: it sounds like you've identified a limitation in your IDM sphere: currently ERP-based person identifier, but if you have multiple ERPs in play, maybe time to use a centralized IGA identifier. *It's OK to have multiple identifiers*, it's just important to have a central, forward identifier
    - Gabor: but you don't need to necessarily make your SPRIDEN ID your choice identifier
        - Kevin: main problem is that there could be 2 of them for the same person on 2 systems, and if they don't agree, we'll have problems, esp since the two ERPs are syncing data (though we've told Ellucian that they can't sync identity data)
        - We have lost some choice since the SPRIDEN ID is everywhere
- Colin: what do student employees look like, as an example of someone who would land in 2 Banners?
    - Kevin: when the two systems sync data, we don't let the two sync identity data; when we deal with change, latest change takes precedence
- Gray: probably obvious to most people in room, but if going down path of centralized, opaque identifier, make sure it's not protected/FERPA related
    - What is the argument that it's FERPA data?
        - Gray: the real reason for pushback we've gotten (from one dept that is claiming the identifier is FERPA data) is that there are some profs that still print out grades, even though that's not supposed to be happening anyway

- Andrew: at UW Madison: central was decided a while ago, but someone had the foresight to call it a PVI (Publicly Visible Identifier). See here for a little more info: https://data.wisc.edu/infoaccess/available-data-views/uw-madison-student-administration/supporting-data-views/id_crosswalk_uwmsn/