Link to 2023 ACAMP Wiki

Advance CAMP Thu. Sept 21, 2023

Room - IV

Session Title: Does it have to be this hard? Eduroam, etc.

CONVENER: Margaret Cullen

MAIN SCRIBE(S): MikeZ, Nicole

ADDITIONAL CONTRIBUTORS: Mary McKee, Rob Carter, Nicole Roy, Matthew Economou, Patrick Radtke, Tom Jordan, Kellen Murphy, Martin D, Drew Capener, Matthew Slowe

# of ATTENDEES: 17

CALL TO ACTION:

InCommon Futures 2 survey link

DISCUSSION:

Came out of CACTI discussions WRT the problem of lowering IT budgets, deployments to smaller HEs, K12s, etc that might lack staffing/expertise on IAM, federated ID, eduroam, etc.

What can we do to make it easier for these members of the community?
Technology? Programs? Documentation? Vendors? Fed. operators?

Kellen M: Was in the Shib community as a consultant, when I joined university staff there was little documentation. So some sort of centralized source of documentation for TAP components?

Martin D: +1 to that, plus documented use cases for the components. Include size of institution, what they chose to deploy and why

Matthew E: WRT documentation, I've been involved with BE, still find it difficult to read through existing docs. Recognize that some of BE is process, but also has technical components, having a source on how to meet each expectation/requirement with more clear delimitation between the process and technical with checklist for each would be helpful. Default TAP components should be linked to clear documentation.
Nicole R: I get what you're saying b ut not sure if that should be a part of BE2?
Matthew: Propose that docs include best current practices for each component, esp for default components. So does it automatically support RNS, etc? We should have an idea of common use/case and build toward that

Kellen: Consider proxying to Azure AD. Links are super helpful, especially to common/basic structures. Wiki is good but requires a certain amount of expertise

TomJ: As we talk about rolling out BE would it be reasonable to set expectations that our documentation is updated to reflect current requirements

Nicole: Consider that people are moving away from Shib (or other components) because it's "too hard", and we've tuned everything toward Shib. We should make it easy to deploy and support foundational components.

MaryM: I think across the industry we're all struggling with differentiation between our products, makes it hard to define our lanes, document and deploy appropriately.

Margaret: So a lot of what we do is Shib focused and not everyone uses Shib?

Consensus: Yes

Margaret: Consider difficulty in keeping eduroam documentation for commercial products like NPS. Often fell out of date, increased support burden for us, made it hard for community to deploy eduroam. So do we want to

?: Keep in mind that we rely on admins to do things correctly - including documentation and tools to deploy correctly is key

Kellen: Keep in mind persistent maintenance and support needed, esp when considering updates to products like Shib. Schools with low/no staff are challenged by version changes, even patches

MattE: Would add that current multilateral ID federation practice involves huge number of frameworks, profiles, etc. with no central info resource. Especially true for SPs - they tend to get lost in the shuffle. Lots of attention/resources given to IdPs by comparison.
Nicole: Also consider impact of SPs that are poorly deployed and supported - even see this in the commercial space.

Matthew Slowe: WRT SP testing we (JISC/UK Federation) have toolbench for SPs to test their deployment. The IdP we test against is in eduGAIN, welcome to make use of it

- UK Federation Test SP: https://test.ukfederation.org.uk
- https://release-check.edugain.org
- UK Federation Test IdP (for SP testing) in edugain as https://test-idp.ukfederation.org.uk/idp/shibboleth (https://met.refeds.org/met/entity/https%253A%252F%252Ftest-idp.ukfederation.org.uk%252Fidp%252Fshibboleth/)

Margaret: Would be great to be able to configure a tool to pass certain attributes to test your SP
MatthewS: Our tool can do some of that - RNS attributes, etc.
Margaret: Would it be good to put up a resource for testing tools for services and components within the community?
COnsensus: Yes

MattE: Getting a list of important relevant standards centralized and present to deployers along with best practices/suggested implementation docs. Something like Seamless Access effort for libraries. I2 wiki is good but still difficult for others to find everything they need.
NicoleR: What about the people who never come to these meetings and read our mailing lists? Also, what about the work that goes into a deployment for basic implementation?

Kellen: Grouper put together documentation packages broken out by “maturity level” - could take similar approach here.
NicoleR: Would be good if components had “maturity level 0” container
TomJ: A significant part of this is more about onboarding new members of our community. We could use more durable artifacts geared toward new people.
RobC: Take an additive approach to maturity level tiers of documentation
MaryM: The right advice at the wrong time is the wrong advice. Sometimes floundering is inevitable or even desirable - something to keep in mind. Scale and scope documentation to each maturity level carefully
RobC: We’ve done a lot to document how things work and how to make them run. Haven’t documented how to use the tools to do things, match to use case. Need to be able to articulate to people how to solve for just their issue

Romy: Curious about the line between documentation and training. Sometimes the training is the best approach, but want to consider how that would be formatted - self paced, instructor lead, etc

Martin: Documentation has been discussed before. I2/InCommon could provide a clearinghouse for documentation. Training goes so far but might not speak to your use case and how to use the tool
NicoleR: Have to consider what training really is. If I have a pile of documentation I can get myself up to speed. Many folks are like that, can be considered “training” and might work best for some folks
Margaret: Could be self paced for basics, have pointers toward
MattE: Is there a Federation version of Stack Overflow? There should be

Margaret: Want to pivot to what I2/InCommon could do to get info to new community members. Work through vendors?
DaveS: I get that identity is hard and people have to learn this stuff. But consider that when we talk about a lack of resources time is one of those things. They might not have time for self paced learning. Don’t often talk about shortcomings on product side but would like to hear about that from this group (and the community at large).
MaryM: The call to action here is to think about how to synthesize and distill - look at product differentiation, look at defining major design considerations
MattE: Agree - focus on good practices, not best practices. Allow for wide differences in needs and resources within the community

Romy: I would ask everyone in this room to fill out the Futures survey - communicate directly with us through that, as that effort is getting a lot of internal attention

InCommon Futures 2 survey link

Margaret: Keep in mind we're going to be taking this question to eduroam Support Organizations, IAMonline, Community Exchange, etc. Want to reach numerous audiences, levels of expertise, different roles of folks from within the community.

TAP Components whiteboard:
[image]

Relevant Guidance and Standards

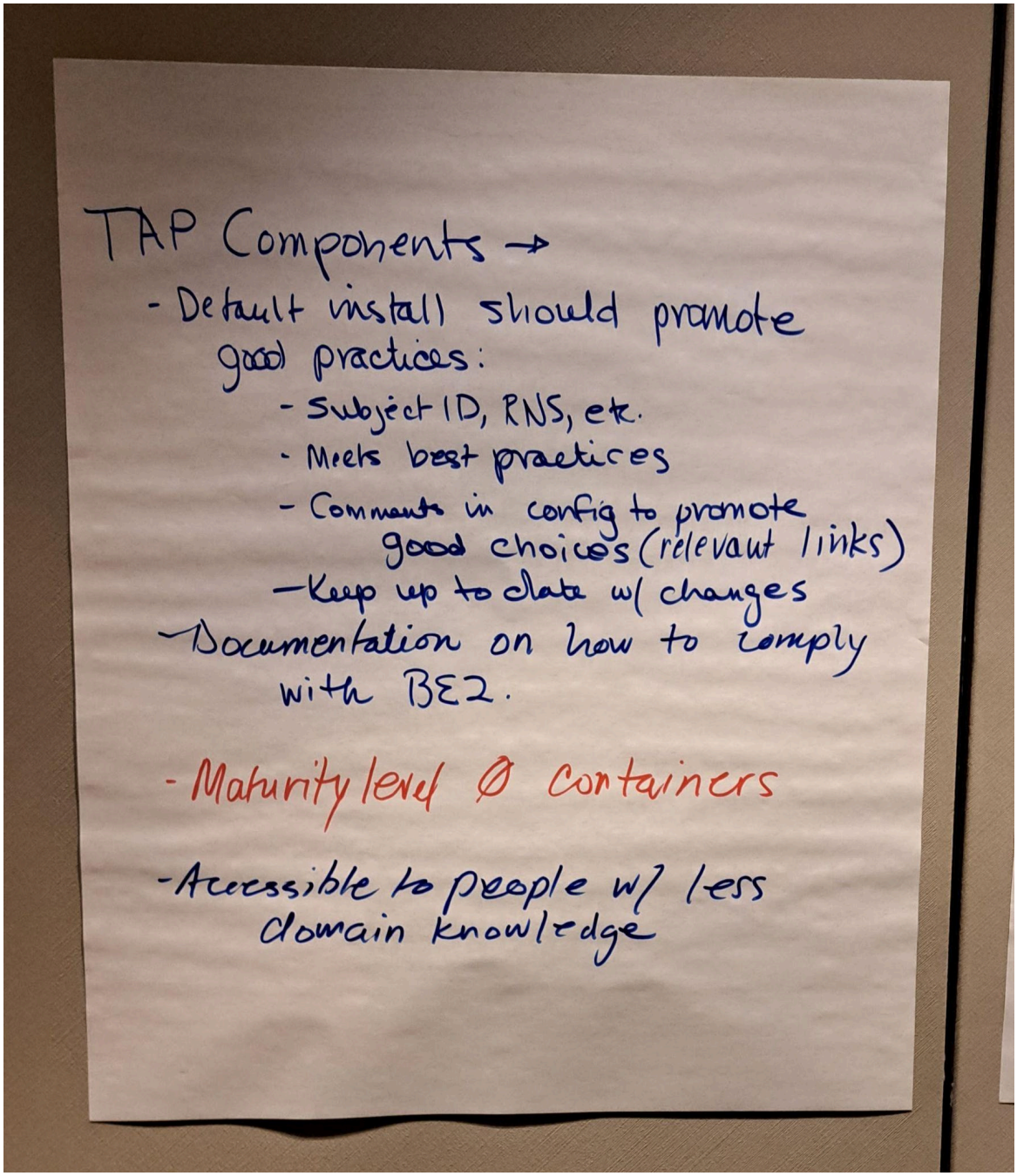
What does "works properly" mean?

This is not a complete list and is not presented in any meaningful order:

- Baseline Expectations for Trust in Federation Version 2
- EDUCAUSE Information Security Guide: Effective Practices and Solutions for Higher Education
- Metadata Query Protocol
- REFEDS Assurance Framework
- REFEDS Multi Factor Authentication Profile
- REFEDS Research and Scholarship Entity Category
- REFEDS Security Incident Response Framework
- REFEDS Single Factor Authentication Profile
- SAML V2.0 Metadata Deployment Profile for errorURL
- SAML V2.0 Deployment Profile for Federation Interoperability Version 2.0
- SAML V2.0 Subject Identifier Attributes Profile
- SeamlessAccess

- SSL Server Rating Guide

ARTIFCTS / LIKS


TAP Components →
- Default install should promote good practices:
- Subject ID, RNS, etc.
- Meets best practices
- Comments in config to promote good choices (relevant links)
- Keep up to date w/ changes
- Documentation on how to comply with BE2.
- Maturity level Ø containers
- Accessible to people w/ less domain knowledge

Documentation / Training

- Grouper, in particular
- TAC components
- Use cases, esp. component interaction (size of inst., how, why?)
- Bulleted list for BE2
  - Make process/tech distinction
  - → Checklist
  - Default install of TAP components should meet Good ~~Best~~ Practices / BE 2
    - ↳ Subject ID/RNS, etc.

A lot of focus on certain implementations (Shib, FreeRadius, etc.) but little information on how to work w/ other vendors (MS NPS, Cisco ISE, Azure AD, etc.)

Docs are IDP-centric

- SPs are critical to having a system that does -anything-

Summary of relevant standards (on Wiki?)

- REFEDS
- IETF Specs
- Seamless Access

Docs based on "maturity level"?

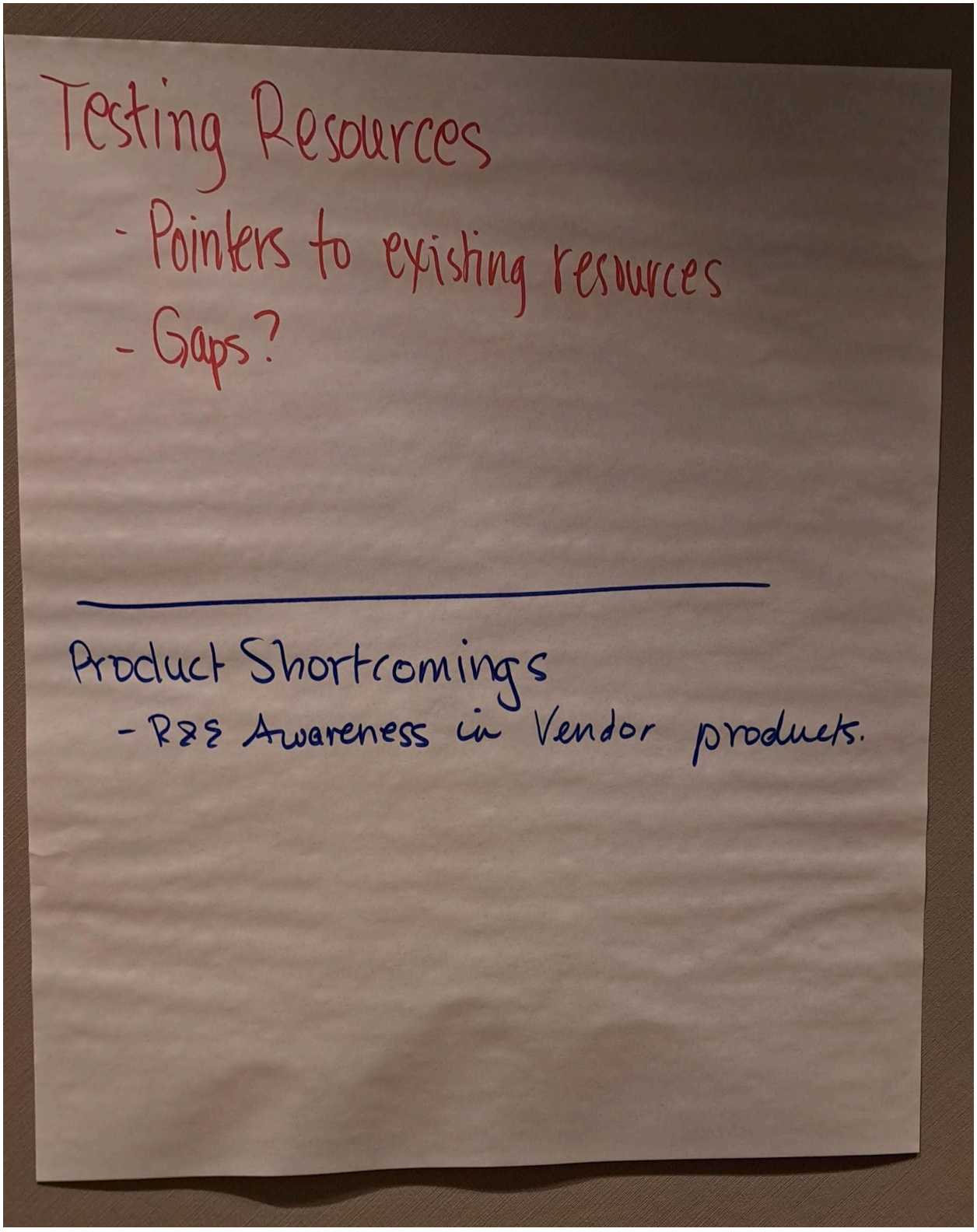
"Durable artifacts" for beginners

- "Right advice at the wrong time is the wrong advice!

Get the community to supply doc., such as use cases, maturity paths, etc.

federation.stackoverflow.com?

"Youtube" videos?


Testing Resources
- Pointers to existing resources
- Gaps?
Product Shortcomings
- R&E Awareness in Vendor products.

linked