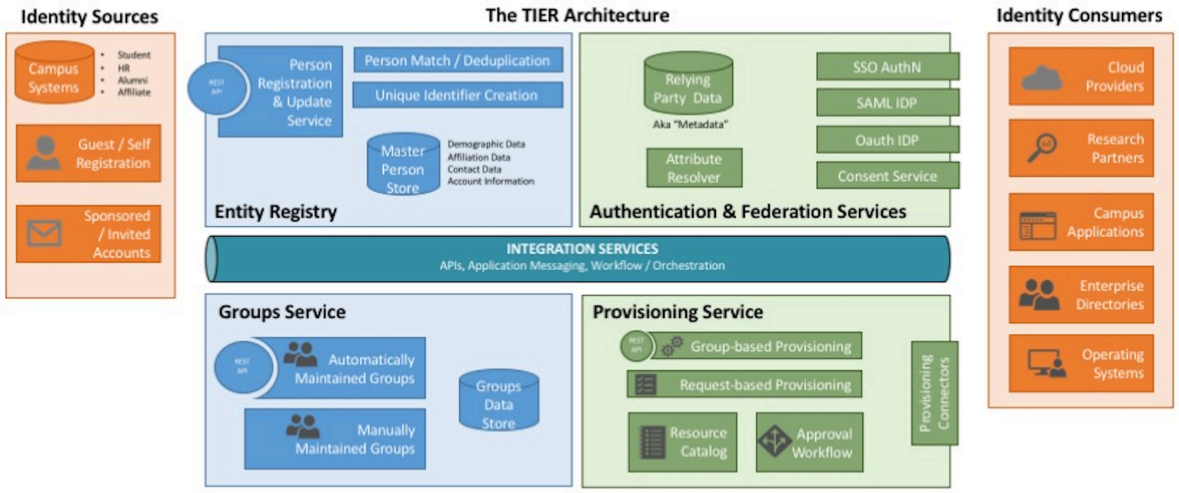
[DRAFT] CACTI Recommendations for improvements to components in TAP

Overview:

CACTI has been asked for recommendations for improvements to the Trusted Access Platform components shepherded by the Internet2 Component Architects group.

The TAP Reference Architecture has logical components illustrated below as well as a detailed list with components.



In detail, current and planned TIER components, related to the reference architecture from the TAP page. A components abbreviation is in square brackets for short reference:

- [PR] - Person Registry -- **COmanage**, **midPoint**
- Authentication & Federation Services
- [IdP] - WebSSO/SAML Identity Provider -- **Shibboleth Identity Provider**
- [MD] - Relying Party Information -- **InCommon Metadata**
- [CS] - Consent Service -- **Scalable Consent**
- [GS] - Groups Service -- **Grouper**
- [PS] - Provisioning Service - **COmanage**, **midPoint**
- [MQ] - Messaging & Queuing Service -- **RabbitMQ**

Example suggestion to cut and paste

Suggestion: Add ability to offer thing .. that..
Component: [IdP]
Estimated effort range: small / medium / big
Estimated impact: <scope>,<small/medium/large>
Submitter: <yourname>
Supporters: <name>,<name>...
Date: Oct 4, 2022

Short Description:

Objective/ Value proposition:

The Suggestions

Suggestion: Add default ability for eduPersonAffiliation calculated from users groups
Component: [IdP]
Estimated effort range: small to med
Submitter: Chris P
Short Description:
eduPersonAffiliation is not often derived from a single directory attribute as the eduPerson objectclass is not as dominant as it once was. To assist sites to better support R&S, it would be valuable to have a bundled example or eduPersonAffiliation calculation that uses a recommended and sustainable form of configuration

Objective: Assist sites to better support R&S upon reference installation.

Suggestion: Add default ability/option SAML proxying as a Shibboleth module enable/disable as calculated from users groups
Component: [IdP]
Estimated effort range: small to med
Submitter: Chris P
Short Description:
SAML proxying has become nearly an essential configuration model that is somewhat predictable and could be created/made into a module that may simplify the configuration experience as well as the sustainment practices around it. By being modular, it can be less a 17 steps thing and many fewer steps.

Objective: Assist sites to use the Shibboleth IdP as a “federation supporting layer” on top of their commercial SSO service (e.g. Azure AD, Okta, …)

Suggestion: Provide a Shibboleth/SSO deployment guide (akin to the Grouper Deployment Guide), or at least a single site with lots of useful “artifacts” for the Shibboleth IdP.
Component: [IdP]
Estimated effort range: medium to large
Submitter: Mike G
Short Description:
This is really building on the first two suggestions above, expanding those into a deployment guide/library of useful articles and artifacts for various Shibboleth IdP deployment use cases. Pull together information on how to use it as a Proxy, how to support the growing number of federation entity categories, subject identifiers versus EPPN and eduPersonTargetedID (and choosing a good underlying attribute for such), a lot more explanatory info/”best practices” on managing NameIDs, examples of configuring for asserting assurance, etc., with a library of configuration examples for all of this. Maybe even federation-distributed versions of various config files etc.

Objective: Assist sites to use the Shibboleth IdP for a variety of different SSO use cases.

Suggestion: Develop community documentation around use cases for CoManage/Grouper/Midpoint in overlapping functionality spaces
Component: [Provisioning] [Registry]
Estimated effort range: medium
Submitter: Rob C.

Short Description:
Community feedback repeatedly suggests there remains confusion about the scenarios in which provisioning and registry management might benefit from different features of CoManage, Midpoint, and/or Grouper. Deployers and architects seem to grapple with decision-making around which of the tools to apply when. While it's not feasible to be prescriptive, some documentation, possibly collected with help from the user community, of use cases where each of the tools has been successfully employed to solve provisioning and registry requirements could help sites make better use of the products.

Suggestion: Ensure compatibility of the person & group registries with recently finalised EduAPI data standard
Component: [Provisioning] [Registry]
Estimated effort range: medium
Estimated impact: large
Submitter: Jeremy Perkins
Short Description:
The newly finalized EduAPI data standard included a lot of work to make the Person data model flexible for internationalisation and future extension. I think it would be worthwhile to ensure compatibility of both the User Registry and Provisioning service with this new data standard. Compatibility with the EduAPI user model could also enable more robust provisioning services in the future (using the EduAPI standard).

URL-> https://www.imsglobal.org/edu-api (note reference to SUNET, may be able to get some background detail)
Q: interesting companion/duplicative to SCIM? This speaks to more data schema beyond eduPerson?(obviously, but to what degree and should this 'dictionary' be across federations [cp]
Comment: If you look at the example diagram near the top of that EduApi page linked to above, you'll see learning specific provisioning to services such as the ID Card system. As noted in the past, you also have the LTI spec passing identity data to linked "learning tools". What we have are separate standards groups coming at identity passing and provisioning standards from different perspectives, with no obvious sign of alignment between the "identity folks" and the "education-focused folks". Just like the Identifier task force that 1EdTech has recently launched, and that I'm participating in (given Unicon is member of 1EdTech, formerly IMS Global). Not sure that there is a "solution", but it seems like more connections with these efforts need to exist. [mag]

Suggestion: Have the ability to manage the Shibboleth IdP in a more web friendly manner rather than CLI.
Component: [IdP]
Estimated effort range: big
Estimated impact: Large
Submitter: Chris Phillips
Supporters: <name>,<name>...
Date: Oct 24, 2022

Short Description:
The Shibboleth idP is a critical item and at this moment in time it is managed via configuration files and has no administrative web interface to interface. This continues to be a barrier to the community as the talent, capability, and desire to work on the CLI is diminishing at an astonishing rate such that sites do not come current.
Objective/ Value proposition:
Offer a more friendly and durable interface to manage the idp and it's complexities. The intent being to simplify some basic common patterns (idp-ldap-openldap,

idp-saml-proxy-passthrough, idp-saml-proxy-augment with ldap) to simplify out of the box usage, admin, and upgrades(aspirational, but main quest is to make it easier.)

Suggestion: Establish a reference *BAC set of reference baseline techniques that can be used ‘out-of-the-box’ such that at least a group based access control model companions the IdP with Grouper / Comanage to allow sites to manage access at scale in basic contexts
Component: [IdP]
Estimated effort range: big
Estimated impact: large
Submitter: Chris phillips
Supporters: <name>,<name>...
Date: Oct 24,2022

Short Description:

Objective: Improve resiliency and robustness of Shibboleth EDS

Suggestion: Add more intuitive error feedback on both implementation and usage
Component: [Authentication & Federation Services]
Estimated effort range: small to med
Submitter: Marina K
Short Description:
When implementing Shibboleth EDS, errors that are generated by this piece of software are not user friendly or intuitive. At times it is not clear what the issues are and what is causing them. For any new organization any usability issues would a deciding factor to implement it or not.

Objective/ Value proposition:

Suggestion: To undertake a few research-esque outcomes for extra strong authentication components for the IdP to attempt to identify implementation challenges on WebAuthN, Passkeys
Component: [IdP]
Estimated effort range: medium
Estimated impact: medium to large
Submitter: Chris Phillips
Supporters: <name>,<name>...
Date: Oct 24, 2022

Short Description: There is little incentive to do the basic ‘can this work and if so, how?’ research on the newer technologies emerging and how they can integrate. If this were undertaken either at Internet2 or more likely in partnership with others like REFEDS or GÉANT it may be possible to prototype/incubate ways to adopt new technology and then ingest it in our supply chain as base features.
Objective/ Value proposition:
To stay current and continue to invest in the identity provider capability at large with more consistency and technical leadership.

Suggestion: To undertake a few research-esque outcomes for Credential Management functionality.
Component: [IdP][midPoint][COmanage]?
Estimated effort range: large
Estimated impact: medium to large
Submitter: Mike Grady
Supporters: <name>,<name>...
Date: Nov 4, 2022

Short Description: (See comment on WebAuthn/IdP suggestion above.) Should Credential Management be brought together in one cohesive application? Password management, MFA device management, WebAuthn device management. Or should those all remain separate, counting on commercial MFA providers to provide all the pieces for MFA, and building/adding something special for WebAuthn? Leaving just password management to the TAP Suite? The only current piece of the TAP suite that has any functionality in this space is the password management that is within midPoint, and maybe Authenticator functionality in COmanage(?). Is the best plan forward to build (separately) on that being functionality provided by midPoint and/or COmanage? Should the Shib IdP provide at least some basic password management functionality? (Unicon has explored adding this to the IdP as an extension/now plugin, adapting work from the CAS Server space.)
Objective/ Value proposition:
Toexplore adding cohesive credential management to the TAP suite of services.

Appendix

Details