Next Steps Compiled from Session notes

Action Items from 2011 Advance CAMP

Note: Follow-up is planned on several action items, as indicated in the Status column. This follow-up will take the form of gentle inquiries, as opposed to regularly scheduled calls and check-ins.

#	Session at Advance CAMP	Description	Lead	Status
1	Rewriting IAM Policies	Establish the TEP (Tools and Effective Practices) wiki space as the home for policy and governance discussions	Michael Pelikan	
	ECP	ScottK will continue work with the Condor group on the ECP-enabled file mover	ScottK	Tom will do some follow-up with leads on the ECP work
	ECP	Add links on the SHIB2/ECP wiki page that point *to* other pages where this nascent ECP interest group's activities can be described. Use those linked pages as a home on the web for ongoing discussions		
	ECP	Collaborate to deliver a Python ECP client module that returns a Python cookie-jar containing session cookies that allow your Python app to keep talking to the SP	Roland, ScottK	
	ECP	Work with Condor group on ECP-enabled file mover	ScottK	
	ECP	Refactor his HPC access via SAML solution to use the ECP approach	Arnie	
	ECP	Suggest to InCommon that they consider recommending that sites protect their ECP endpoint on the IdP with X.509 certs. Otherwise there will be as many varieties of protection as there are ECP endpoints.	ScottK (and others?)	
	ECP	Document other ECP clients and how you use them PAM/Shib	requested by Todd Picket	
	ECP	Create an ECP Reading list / tutorial	not assigned	
	Multiple Attribute Stores and Shib IdP	Create documentation on the use of attribute aggregation. Get input on the multi-datastore handling by the IdP. Big question is how to handle multiple data sources connected to an IdP.	Mike Wiseman & Steven Carmody	RL "Bob" will do some follow-up with leads
	OAUTH	ACAMP Prog. Committee should encourage the Social ID working group to deal with these issues: - Look forward to CAS OAuth support. - Look forward to finalization of OAuth 2.0 and stabilization of the OAuth protocol. - Gain more experience using OAuth with apps	Social ID WG	
	Permissions Mgmt UX and UI	ACAMP Prog. Committee needs to encourage the MACE-paccman WG to address the items that emerged, including: • [TomZ]: Mock up a UI...* • [All]: Bring selected UX/UI Business Analysis experts at our institutions into the ongoing conversation * • [KeithH] Create child wiki pages off the "MACE-Paccman" site. Adopt "Permissions Management UX/UI" as an ongoing Paccman work item and as a regular agenda item for Paccman conference calls. Supplement the "Canonical Use Cases with Solutions" with material from this group's work.* • [KeithH] Contact Nils about what Surfnet Conext and COIN offer and about his willingness to participate in these discussions* • [MichaelG] Draft a mini-charter for an effort to develop something like an RFP for a Permissions Management UI/UX Package	MACE-paccman	
	InCommon Silver Certification	Facilitate discovery of InCommon Silver work and sharing community work -- facilitate outreach on community outreach and outcomes InCommon to • develop a list of campuses implementing InC IAPs • create a mailing list of folks implementing InC IAPs who wish to share ideas • announce when a campus becomes Silver (or Bronze) compliant on the InC Participants list • create an implementation wiki to include case studies and community-driven implementation FAQ	Ann West	
	Making Services Discoverable to Users	ACAMP Prog. Committee needs to follow up with Michael and Roland to discuss concrete action items. (Establish standards for storing info? Work with SWITCH on this? Establish a service catalog?)	MichaelG and Roland	RL "Bob" will do some follow-up with leads
	Identify Gaps in IdM	Ensure that a secure environment exists to have discussions about vendor products.		
	Identify Gaps in IdM	Berkeley and FIFER work together to develop some documentation for the community.		
	Identify Gaps in IdM	Identify people who can answer people about different IdM systems. (Use cases, user storeis are more useful than features in a grid.)		
	Social Identities in R&E	Migrate from "OPENID" wiki space to "Social Identity" wiki space	SteveO	
	Social Identities in R&E	Create a listing of what people are doing and track what the standards are in the higher ed environment	Steven and the Social ID working group	
	LDAP Options, SubTrees, and Composite Attributes for Identity	Send writeup of issue statement for "eP[Scoped]PAeP"	Todd Piket	
	LDAP Options, SubTrees, and Composite Attributes for Identity	Ask Rob Carter for permission to use the 389DS plugin that he & Michael Gettes wrote to handle Kerberos "the right way".	Delegate this to MACE-Dir	

COMPLETE LIST OF ACTION ITEMS FROM THE BREAKOUT SESSION NOTES

ECP Session

ACTIVITIES GOING FORWARD / NEXT STEPS

https://wiki.shibboleth.net/confluence/display/SHIB2/ECP is the home for Shibboleth work around ECP support

[All] Add links on the SHIB2/ECP wiki page that *point to* other pages where this nascent ECP interest group's activities can be described. Use those linked pages as a home on the web for ongoing discussions

[Roland Hedberg, Scott Koranda] collaborate to deliver a Python ECP client module that returns a Python cookie-jar containing session cookies that allow your Python app to keep talking to the SP

[Arnie] Refactor his HPC access via SAML solution to use the ECP approach

[ScottK] working with Condor group on ECP-enabled file mover.

[ScottK and all] Suggest to InCommon that they should consider recommending that sites protect their ECP endpoint on the IdP with X.509 certs. Otherwise there will be as many varieties of protection as there are ECP endpoints.

- [Friday morning "ECP Continued" discussion|display/ACAMPIdSummit2011/ECP+the+discussion+continues||||||||]: X.509 may be too limiting. Basic Auth use cases (Live@EDU) are common.
    - Multiple ECP endpoints? One for X.509 and one for Basic Auth?

REQUESTS:

- Todd Picket: Document other ECP clients & how you use them: PAM/Shib
- ECP reading list, tutorial??

Dealing with Multiple Attribute Stores and the Shib IdP

ACTIVITIES GOING FORWARD / NEXT STEPS

1. Document the use of attribute aggregation.

2. Get input on the multi-datastore handling by the IdP from IdP developers.

Grouper Permissions Allow/Deny

ACTIVITIES GOING FORWARD / NEXT STEPS

- Looking at agreeing on adopting one of the simpler UI's? - Status of maturity of API's?
- What are the use cases for this?

SPs Over-Trusting Weak Identities, What to Do?

ACTIVITIES GOING FORWARD / NEXT STEPS

- Perform or complete a classification of confidential data at the institution.

- Where possible, require a risk assessment from any unit using authentication information.

- Where possible, gather information after the fact about sites using authentication information.

- Where possible, gather information after the fact about sites using authentication information.

- Have a conversation about VPN and level of assurance at the institution, come to an understanding and publish it.

- Repeat for services other than VPN.

OAUTH

ACTIVITIES GOING FORWARD / NEXT STEPS

- Look forward to CAS OAuth support.
- Look forward to finalization of OAuth 2.0 and stabilization of the OAuth protocol.
- Gain more experience using OAuth with apps

Roles Vs Groups Rematch

ACTIVITIES GOING FORWARD / NEXT STEPS

- Finding a common space where we can throw up doc from campuses that have done significant role engineering
- Campuses using Grouper should share how they are establishing/defining groups vs roles, and push towards a common ground

FIFER API

ACTIVITIES GOING FORWARD / NEXT STEPS

1. Need to figure out best way to move forward WRT preferred approach for Group Web Service aka Alternate Demo Plan Mock-ups
2. FIFER needs project player (FIFER API consumer) input, but also those in VO/CO space

Permissions Mgmt UX and UI Issues

ACTIVITIES GOING FORWARD / NEXT STEPS

[TomZ]: Mock up a UI...

[All]: Bring selected UX/UI Business Analysis experts at our institutions into the ongoing conversation (SteveC: Their first question is gonna be "What are your requirements?" (knowing laughter from the audience)

[KeithH] Create child wiki pages off the "MACE-Paccman" site. Adopt "Permissions Management UX/UI" as an ongoing Paccman work item and as a regular agenda item for Paccman conference calls. Supplement the "Canonical Use Cases with Solutions" with material from this group's work.

[KeithH] Contact Nils about what Surfnet Conext and COIN offer and about his willingness to participate in these discussions

[All] Email hazelton@wisc.edu if you are interested in participating in ongoing work

[MichaelG] Draft a mini-charter for an effort to develop something like an RFP for a Permissions Management UI/UX Package

CIC InCommon Silver Certification

ACTIVITIES GOING FORWARD / NEXT STEPS

InCommon to

- develop a list of campuses implementing InC IAPs
- create a mailing list of folks implementing InC IAPs who wish to share ideas
- announce when a campus becomes Silver (or Bronze) compliant on the InC Participants list
- create an implementation wiki to include case studies and community-driven implementation FAQ

Buildling Partnerships between Research and IT (IdM)

ACTIVITIES GOING FORWARD / NEXT STEPS

- Sharing of U of Toronto's document.
- Sharing of the job descriptions of the Customer Relations Manager, or the central IT research support staff member

Making Services Discoverable to Users

ACTIVITIES GOING FORWARD / NEXT STEPS:

- See what Switch, others are doing to avoid duplicating effort
- Look for standards for storing information
- Needs to accommodate more than Shib, InCommon
- Service catalog type approach?

Federated ID for Research Applications

ACTIVITIES GOING FORWARD / NEXT STEPS

- ECP work for science applications. Technical work first, then encouraging adoption by InCommon campuses.

Identify Gaps in IdM

ACTIVITIES GOING FORWARD / NEXT STEPS

- Secure environment to have discussions about vendors products
- Berkeley and FIFER work together to put some documentation out.
- Identify people who can answer questions about different IDM systems
- Use cases, user stories more useful than features in a grid.

What Can/Should Grouper Do for Me in ReFactoring my Institution's Group Management?

ACTIVITIES GOING FORWARD / NEXT STEPS

- UBC may post information to the wiki regarding their use case -- DONE, see https://spaces.at.internet2.edu/display/Grouper/The+University+of+British+Columbia;

SP OnBoarding

ACTIVITIES GOING FORWARD / NEXT STEPS

- uApprove adoption (support work already in progress on this)
- discussion of central InCommon services
- REFEDS WG

Provisioning

ACTIVITIES GOING FORWARD / NEXT STEPS

- EDUCAUSE IdM list for collaboration
- provision@internet2.edu (development)
- who is rolling your own ? UBC, Yale, Texas A&M, ?

Social Identities in R&E

ACTIVITIES GOING FORWARD / NEXT STEPS

SteveO to Migrate SocialIdent wiki space to get out from under the "OpenID" label.

GFIPM (Global Federated Identity and Privilege Management)

ACTIVITIES GOING FORWARD / NEXT STEPS

-Look at cloud initiative work on standardizing schemas and offer in put
-May not fit in this category--reports on progress/status are of interest

Web Service for IAM

ACTIVITIES GOING FORWARD / NEXT STEPS

- Continued work toward standardizing web service calls and, potentially, message formats (e.g., JSON, XML, SOAP).
- Work together to summarize the current landscape, review existing products, identify gaps. (Where does this get done?)

LDAP Options, SubTrees, and Composite Attributes for Identity

ACTIVITIES GOING FORWARD / NEXT STEPS

[Todd Piket] Send writeup of issue statement for "eP[Scoped]PAeP"

[Roland, MichaelG, Keith] Writeup The Options: 1) Why would you ever want to do this in LDAP? attr. options, composite attributes, sub-entries, ... Start with use cases. Bake-off.

[Keith] Ask Rob Carter for permission to use the 389DS plugin that he & Michael Gettes wrote to handle Kerberos "the right way".