U.S. ARF / CICoE Pilot / Trusted CI Identity Management (IdM) Engagement

John Haverlack
R/V Sikuliaq
College of Fisheries and Ocean Sciences
University of Alaska Fairbanks

Josh Drake
Ci CoE Pilot/Trusted CI
Indiana University Center for Applied Cybersecurity Research

Ryan Kiser
Trusted CI
Indiana University Center for Applied Cybersecurity Research

CI CoE Pilot

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI Logon

COmanage™
ARF IdM Engagement Plan

https://docs.google.com/document/d/1Btb4VRaXrZzg_8brZ_vlSMy20PNH-AlcTnamwwr22Ss/edit

May - October 2020

- **Milestone 1:** Catalog Current State of IdM in the ARF
- **Milestone 2:** Recommend an IdM solution
- **Milestone 3:** Proof of concept IdM solution
Objectives of a Federated IdM Service

This engagement explored how to:

- Provide an Opt-In per vessel per service IdM Solution
- Centralized Identity Management capability for the Fleet
- Facilitate Auditability of Authentication Events
- Monitor expired or inactive accounts for deactivation
- Reduce use of shared password accounts
- Leverage Institutional Identity Providers rather than creating new identities
- Streamline On/Off Boarding Processes
- Develop a Shipside Authentication Appliance
IdM Primer Video

https://youtu.be/rZWOXeOsN6E

IdM Primer Presentation

https://docs.google.com/presentation/d/1_rLUbkQYiqvOsPXezn3GLwehj1WEWLwfiELo4qwxie/edit?usp=sharing

- Authentication
- Authorization
- Authentication Services
- Auditability
- Shared Accounts
- Federated Identity Services
Milestone 1: State of IdM in US ARF - Survey Results

- 10 Institution Responded / 15 Vessels Represented
- 60% don’t know how many Institute accounts are accessed each year
- 50% don’t know how many Transient accounts are accessed each year
- 80% don’t know how many inactive accounts are enabled
- Shared Password Roll Accounts are commonly used
- Majority of Credentials are managed locally on each device
- A small number of vessels use AD/LDAP
- End users are storing passwords insecurely
- 60% have only local system logs / 20% have centralized logging
- 10% regularly audit logs
- Majority require strong passwords / 30% use 2FA
- There is a mix of processes for adding / removing accounts
Milestone 1: State of IdM in US ARF

Survey Respondents:
- Support Federated IdM for Cruise Planning, Captive Portal, Science Logging, and File Sharing
- Are mixed or do not support Federated IdM for Email, Kiosks, VDI, SysAdmin, Ops Tech, Vessel Maintenance
- Agree that Federated IdM should never block logins if the Internet is down
- Strongly desire the ability to administer identities from vessel networks
- Agree that federated IdM will be opt-in on a per vessel per service basis
Milestone 2: Recommended Solution
Milestone 3: Proof of Concept

How far did we get?

- Working InCommon / Google Federation
- Working ARF COManage Instance
- Partial Open LDAP Server
- Incomplete AD Server
- Incomplete Samba Client
## USARF People

### Filter

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Josh Drake</td>
<td>Active</td>
<td>No Title</td>
</tr>
<tr>
<td><a href="mailto:drakejc@iu.edu">drakejc@iu.edu</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>John Haverlack</td>
<td>Active</td>
<td>No Title</td>
</tr>
<tr>
<td><a href="mailto:jehaverlack@alaska.edu">jehaverlack@alaska.edu</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ryan Kiser</td>
<td>Pending Confirmation</td>
<td>No Title Pending Confirmation</td>
</tr>
<tr>
<td></td>
<td>Duplicate</td>
<td>No Title</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Duplicate</td>
</tr>
</tbody>
</table>

### Actions

- [Edit](#)
### Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Open</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO:admins</td>
<td>USARF Administrators</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
<tr>
<td>CO:COU:Science Particles:admins</td>
<td>Science Parties Administrators</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
<tr>
<td>CO:COU:Science Particles:members:active</td>
<td>Science Parties Active Members</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
<tr>
<td>CO:COU:Science Particles:members:call</td>
<td>Science Parties Members</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
<tr>
<td>CO:COU:UNOLS Staff:admins</td>
<td>UNOLS Staff Administrators</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
<tr>
<td>CO:COU:UNOLS Staff:members:active</td>
<td>UNOLS Staff Active Members</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
<tr>
<td>CO:COU:UNOLS Staff:members:call</td>
<td>UNOLS Staff Members</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
<tr>
<td>CO:Coowners</td>
<td>USARF Active Members</td>
<td>Closed</td>
<td>Active</td>
<td><img src="edit" alt="View" /></td>
</tr>
</tbody>
</table>
## Enrollment Flows

<table>
<thead>
<tr>
<th>Name</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invite a collaborator</td>
<td>BEGIN</td>
</tr>
<tr>
<td>Link another account</td>
<td>BEGIN</td>
</tr>
<tr>
<td>Self Signup With Approval</td>
<td>BEGIN</td>
</tr>
</tbody>
</table>

Display **25** records. GO

Page 1 of 1, Viewing 1-3 of 3
### COUs

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Science Parties</td>
<td>A container for identities belonging to members and researchers associated with science parties.</td>
<td><img src="edit.png" alt="Edit" /> <img src="delete.png" alt="Delete" /></td>
</tr>
<tr>
<td>UNOLS Staff</td>
<td>Container object for identities permanently associated with UNOLS or the ARF.</td>
<td><img src="edit.png" alt="Edit" /> <img src="delete.png" alt="Delete" /></td>
</tr>
</tbody>
</table>

Display 25 records GO

Page 1 of 1, Viewing 1-2 of 2
## COUs

<table>
<thead>
<tr>
<th>Name</th>
<th>Parent COU</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Science Parties</td>
<td></td>
<td>A container for identities belonging to members and researchers associated with science parties.</td>
<td><img src="Edit" alt="Edit" /> <img src="Delete" alt="Delete" /></td>
</tr>
<tr>
<td>UNOLS Staff</td>
<td></td>
<td>Container object for identities permanently associated with UNOLS or the ARF.</td>
<td><img src="Edit" alt="Edit" /> <img src="Delete" alt="Delete" /></td>
</tr>
</tbody>
</table>

Display **25** records GO Page 1 of 1, Viewing 1-2 of 2
Challenges

- Identity Management is Complicated
- There is more than one way to organize identity data
- Integrating authentication systems is hard
- Bi-directional administration (ship to shore) is not currently available
- CILogon annual subscription: ~$9,000 per year

There are resources that can help us.
Next Steps

● Write a **Federated Identity Management Service** Proposal
  ○ Available to U.S. ARF on a **per vessel / per service Opt-In** basis
  ○ Would pursue potential collaborations with
    ■ CILogon
    ■ CICoE
    ■ Trusted CI
    ■ Marine Facilities Planner (IdM Client)
  ○ Request funding to establish and run IdM service for 5 years