

2015-06-24 - WebAccessControl Authorization Delegate Planning Meeting

Time/Place

- Time: 2:00pm Eastern Daylight Time US (UTC-4)
- Call-in: DuraSpace conference line
 - 1-209-647-1600, 117433#

Attendees

- [David Wilcox](#)
- [Andrew Woods](#)
- [Jared Whiklo](#)
- [Unknown User \(acoburn\)](#)
- [Nick Ruest](#)
- [Joshua Westgard](#)
- [Stefano Cossu](#)
- [John Bell](#)
- [Bethany Seeger](#)
- [Ben Wallberg](#)
- [Julie Allinson](#)

Agenda

Related documents:

- <https://www.w3.org/wiki/WebAccessControl>
- <https://github.com/duraspace/pcdm/wiki#webacl>
- [Authorization Delegates](#)
- <http://www.w3.org/ns/auth/acl>

1. Introduction and topic summary
 - a. Establish common understanding of function of WebAccessControl Authorization Delegate
 - b. Use-cases
 - c. Compile initial requirements
2. Workplan and timelines
 - a. Development, testing and validation
3. Next steps
 - a. Summarize and Post use-cases and requirements
 - i. Iterative meetings, as required
 - ii. Set deadline for feedback
 - b. Create strawman design
 - i. Set deadline for feedback
 - c. Confirm commitments
 - i. developer and stakeholders (verification)
 - d. Schedule sprints

Minutes

Intro and topic summary

- Use cases for WebAC
 - University of Maryland
 - Some resources are public and some are not
 - For public resources, users should not be challenged for authentication
 - Probably not related to authorization but this can be a requirement for WebACL implementation
 - Art Institute of Chicago solves this problem by using a public mirror of the repository
 - Use properties other than `rdf:type` to make assertions about authorization
 - Multiple applications connecting to Fedora and one authorization layer
 - External applications should be able to enforce Fedora WebACLs
- Why do people want WebACL vs. another authorization scheme?
 - Simpler/cleaner than XACML but not as granular
 - Are there use cases in XACML that need to be represented in WebACL?
- How are multiple multiple policies on the same resource interpreted?
 - This would be a matter of implementation
- WebAC permissions

- Read, Write, Append, Control
- Append may be analogous to PATCH, no DELETE allowed
 - Use case: Dropbox functionality for adding resources but not editing/deleting them
 - Use case: Allow users to add new objects to a collection without being able to delete the collection
 - Users can edit/delete their own objects but not the collection
- Granularity
 - Both containers and binaries should support WebAC
 - Should WebAC also support restrictions on properties?
 - Not currently supported in other authorization schemes.
 - Not a requirement for initial implementation
- Authentication
 - Fedora assumes that incoming requests have already been authenticated.
- Web IDs
 - Agents/principals have URIs
 - Currently principals only need to be represented by a string
 - Shibboleth with provide URIs, other authentication systems likely will as well
 - We should support both URIs and strings

Next steps

- Commitments
 - Use cases
 - [Joshua Westgard](#)
 - [Stefano Cossu](#)
 - Development
 - [Peter Eichman](#)
 - [Mohamed Mohideen Abdul Rasheed](#)
 - [Jared Whiklo](#)
 - Testing and verification
 - [Joshua Westgard](#)
 - [Stefano Cossu](#)

Actions

- Collect use cases
 - Post to community and ask for feedback
 - Schedule another call if required
- Check with Hydra community regarding requirements
- Schedule implementation meeting
- Schedule development sprints