Assignment D3: Security Policy

Design an access control policy, including authentication and authorization, to satisfy the security requirements of your D1 system.

* Describe the policy in natural language and ensure that it is not ambiguous.

* Formalize the design of the policy in your favorite (web) programming language. That is, formally define the authentication and authorization (access control) rules as predicates on the data model of your system. See the WebDSL rules in the slides of lecture 6 as inspiration; but use a programming language of your choice to implement the formalization.

Submit a report (in PDF) with your natural language and formal descriptions of the policy. In your report, discuss the following questions:

* Can you separate policy from implementation (through a policy language)?

* How close is your formalization to the description?

* Can it be used as (user) documentation for the policy?

* Can you verify that the formalization implements the design?