UNIFIED AUTHORIZATION PLAN

caBIG Clinical Trials Suite – 20 May 2010

OVERVIEW

AS OF SUITE 2.1

- Authentication is common via caGrid WebSSO
- Authorization is not:
  - Suite applications define their own sets of roles according to their historical use cases and customer feedback
  - User authorization levels are provisioned separately in each application

GOALS FOR 2.2

- Ease adoption by reducing setup and admin costs
- Support hosted deployments for the full suite
- Enable authorization (instead of just authentication) for existing inter-application grid services
- Further integrate the suite applications by harmonizing user roles

TECHNICAL REQUIREMENTS

- Single source/sink for authorization information in the suite
  - Users
  - Business roles
  - Role scopes (site, study, neither, or both)
- High-performance scoped authorization for both single elements and sets

APPROACH OVERVIEW

- Harmonize roles and role scopes with guidance from CTMS subject matter experts in accordance with the business architecture model

- Centralize authorization data in a single CSM 4.2 instance & application

- Provision users uniformly from all apps per their existing creation & association workflows

- Ensure that all access to / updates of authorization information is via the CSM API

TECHNICAL DESIGN

SINGLE CSM FOR AUTHORIZATION

- Centralizes authorization data
- Provides a shared, uniform API for both provisioning and access
- With some enhancements, meets our performance requirements for pre-filtering large data sets

ROLES AND PRIVILEGES IN 2.2

- Application analysts, with input from SMEs, have built a harmonized list of 23 roles and their scopes
- In 2.2, the conceptual mapping from the role description to actual application behaviors is the responsibility of each application
- The way we are using CSM will allow us to represent fine-grained privileges in the central authorization repository in a future version if use cases merit it

CSM MODEL USE – LOOKUP DATA

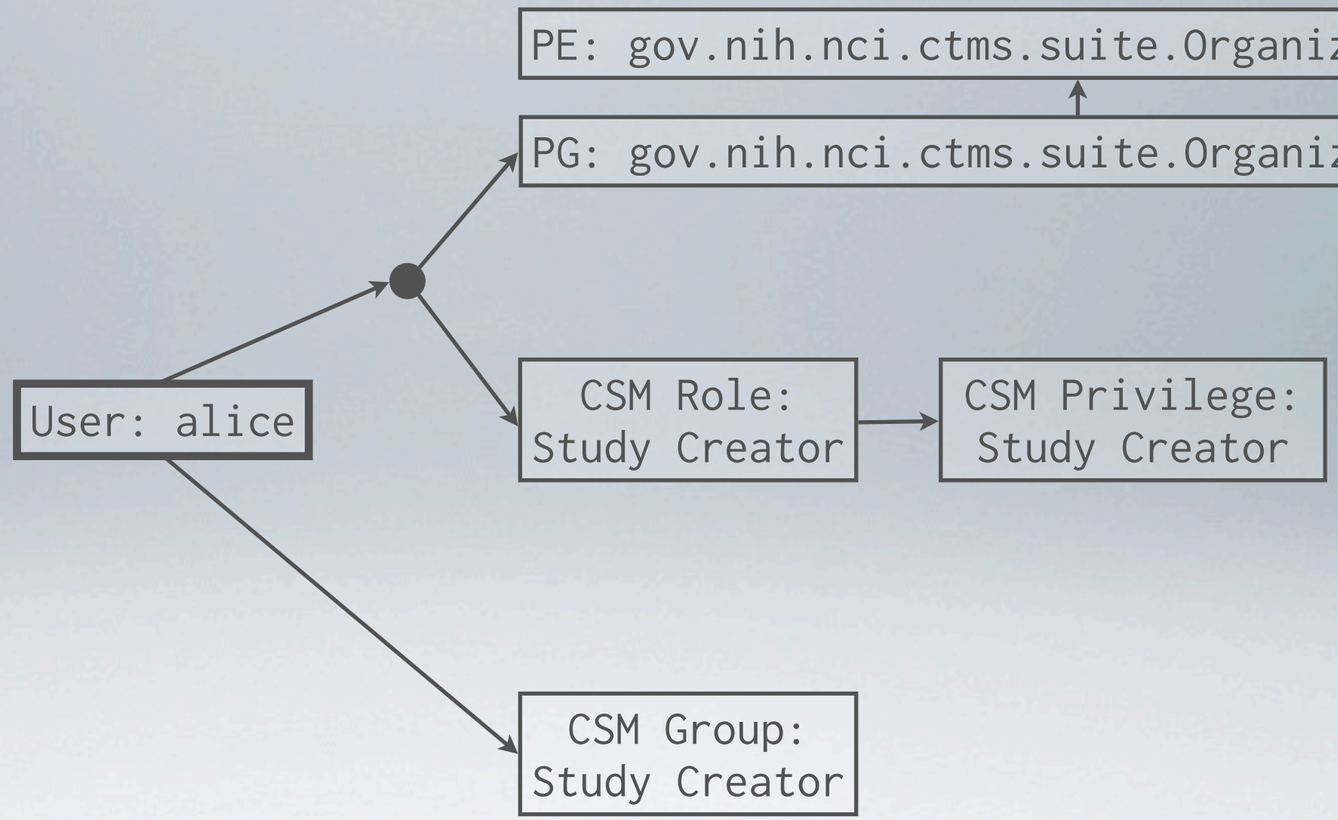
- One CSM application for the entire suite
- Scope objects (sites and studies) each have a protection group / protection element 1:1 pair
  - There are also PG-PE pairs meaning "all sites" and "all studies"
- Business roles are represented by a CSM 1:1:1 triple of group, role, and privilege

CSM MODEL USE – PROVISIONING

- Users are provisioned into the CSM group(s) corresponding to the business role(s) they have
- For scoped business roles, users are further provisioned with a user-role-PG association for each scope object to which they have access
  - Users in the group for a scoped business role but with no role-associated PGs effectively do not have that business role

CSM MODEL USE – EXAMPLE

Consider a user named Alice. She is a *Study Creator* for Northwestern University



CSM PERFORMANCE

- CSM 4.2 provides APIs to do bulk access to a user's protection element / privilege matrix
- However, the provided implementation is much too slow when there are many protection elements in the system
- Fortunately, we can subclass AuthorizationManager and replace the slow query with one that's tuned for our use of CSM

APPLICATION RESPONSIBILITIES

- Use CSM API for all authorization operations
- Robustly handle users which are provisioned by other applications
- Transparently either use or create PG-PE pairs for scope objects when provisioning