HealthSec '12 AUGUST 6-7, 2012 BELLEVUE, WA
3rd USENIX Workshop on Health Security and Privacy
usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Development of a System Framework for Implementation of an Enhanced Role-Based Access Control Model to Support Collaborative Processes

Hung Le, PhD and Dongwen Wang, PhD
University of Rochester Medical Center
Rochester, NY 14642

Outline

- Objectives
- Overview of the EnhancedRBAC model
- System framework for implementation
- Access policy encoding and interpretation
- New York State HIV Clinical Education Initiative (CEI)
- Evaluation
- Discussion
- Conclusion

Objectives

- History
  - Access Matrix (Lampson 1969)
  - Rule-Based Access Control (LaPadula 1973)
  - Discretionary Access Control (DAC) and Mandatory Access Control (MAC) (DoD, 1973)
  - Role-based Access Control (Sandhu 1996)
  - Attribute-based Access Control (Chen 2011)
  - Temporal Role-based Access Control model (Bertino 2001)
  - And many others (Motta 2003; Ni 2010; etc.)

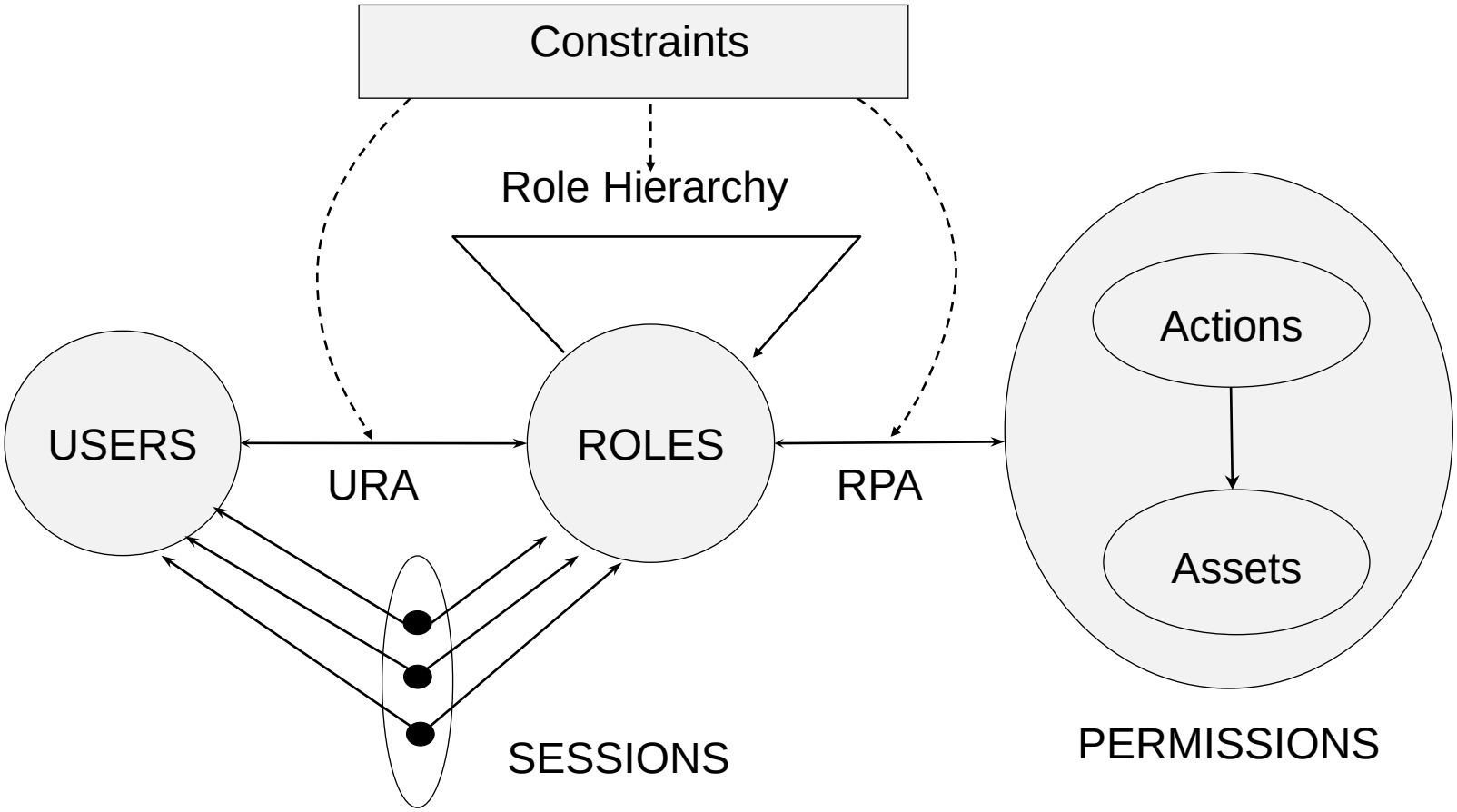
Objectives (2)

- Limitations of existing work
  - Few of these works have addressed information access management in the context of team collaboration and workflow
  - Neither have them been applied for coordination of clinical education programs

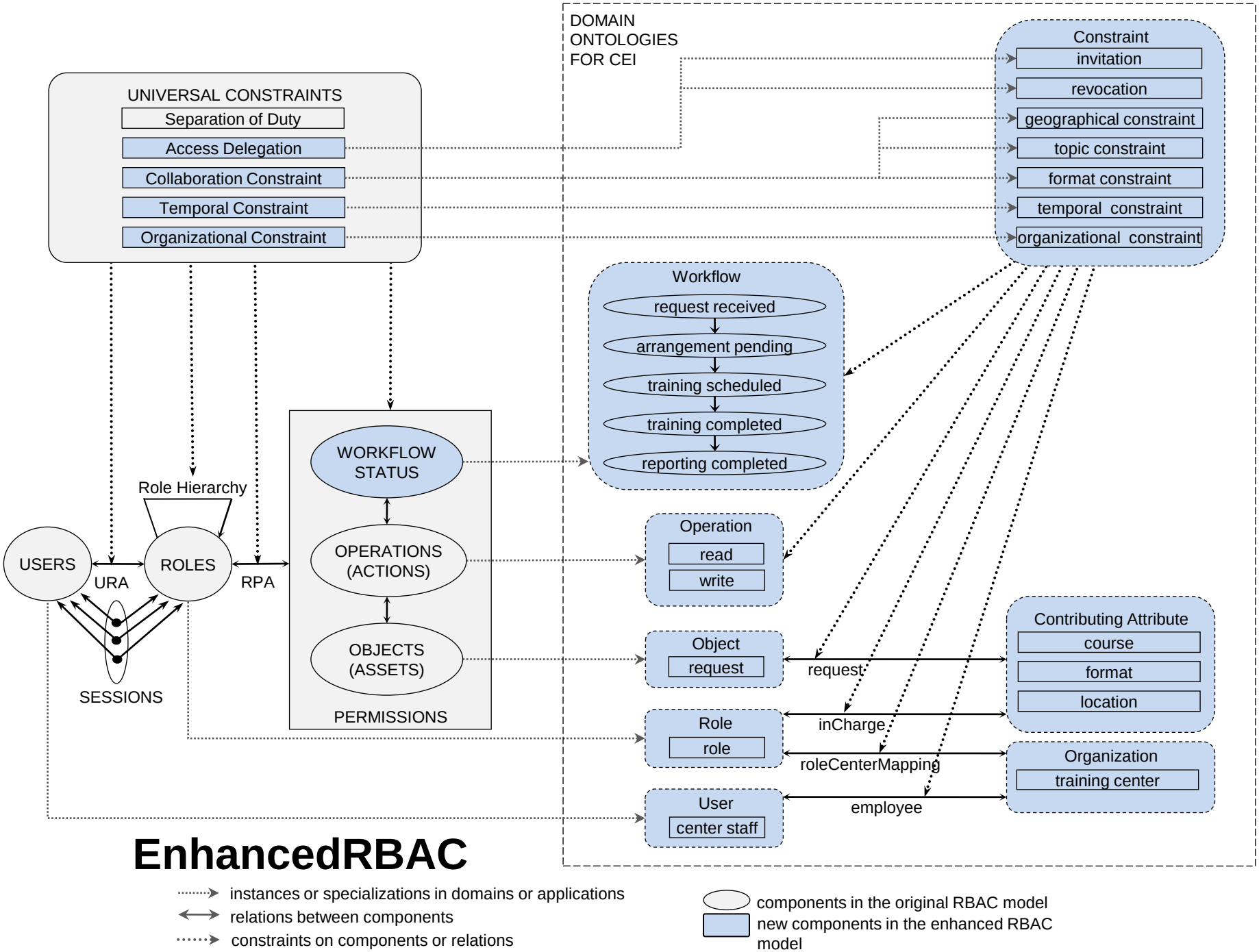
EnhancedRBAC Model

- Universal constraints
- Permission
  - object, operation, workflow status
- Collaboration
  - Bridging entity
  - Contributing attributes
- Domain ontologies

Le XH, Doll T, Barbosu M, Luque A, Wang D.; An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow. *J. Biomed Inform,* 2012 (in press)

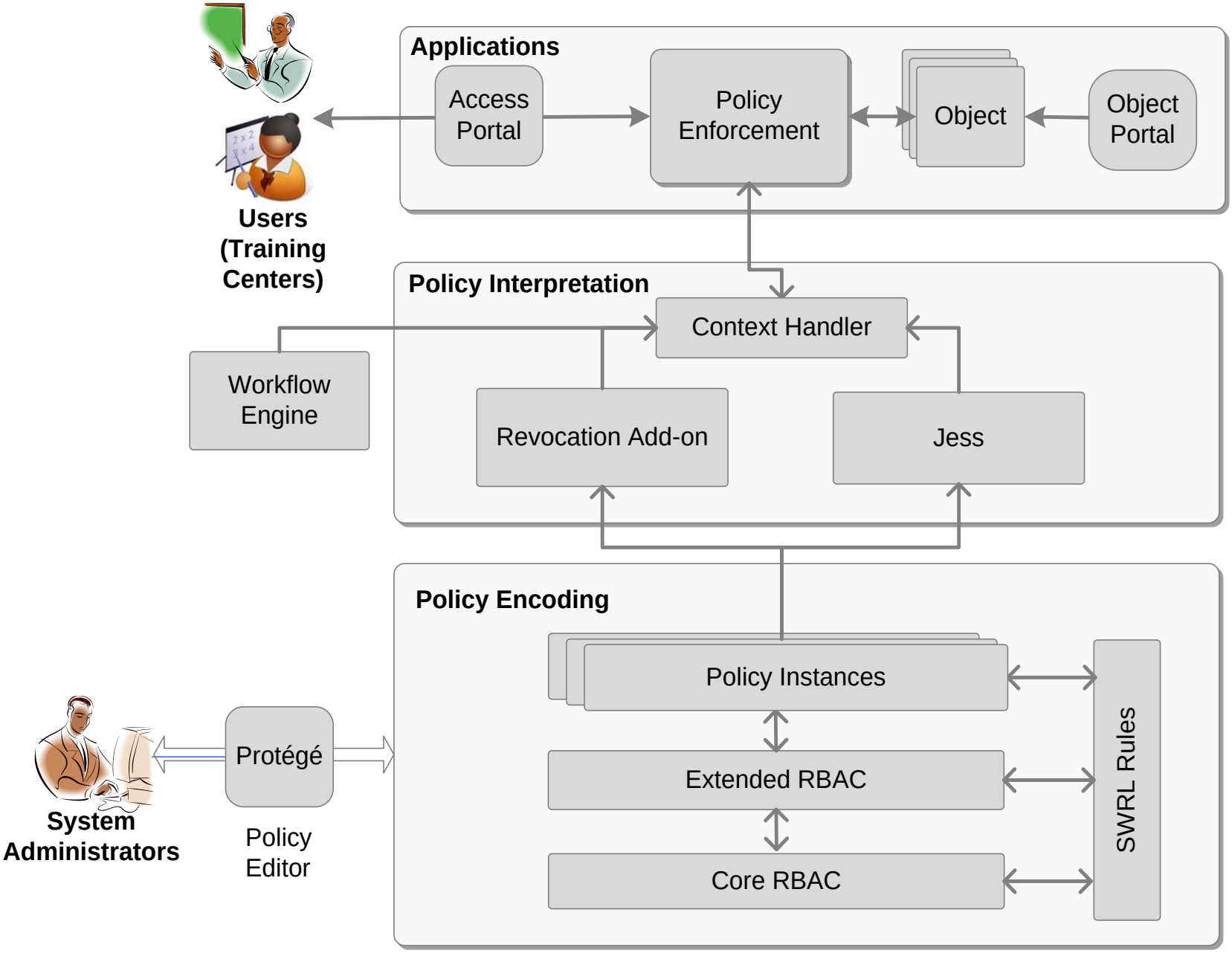


Role-Based Access Control (RBAC) (Sandhu 1996)


DOMAIN
ONTOLOGIES
FOR CEI
Constraint
invitation
revocation
geographical constraint
topic constraint
format constraint
temporal constraint
organizational constraint
UNIVERSAL CONSTRAINTS
Separation of Duty
Access Delegation
Collaboration Constraint
Temporal Constraint
Organizational Constraint
Workflow
request received
arrangement pending
training scheduled
training completed
reporting completed
Role Hierarchy
USERS
ROLES
URA
RPA
SESSIONS
WORKFLOW STATUS
OPERATIONS (ACTIONS)
OBJECTS (ASSETS)
PERMISSIONS
Operation
read
write
Object
request
Role
role
User
center staff
request
inCharge
roleCenterMapping
employee
Contributing Attribute
course
format
location
Organization
training center
EnhancedRBAC
instances or specializations in domains or applications
relations between components
constraints on components or relations
components in the original RBAC model
new components in the enhanced RBAC model

System Framework for Implementation

- Three-layer approach
  - Policy Encoding layer
  - Policy Interpretation layer
  - Application layer

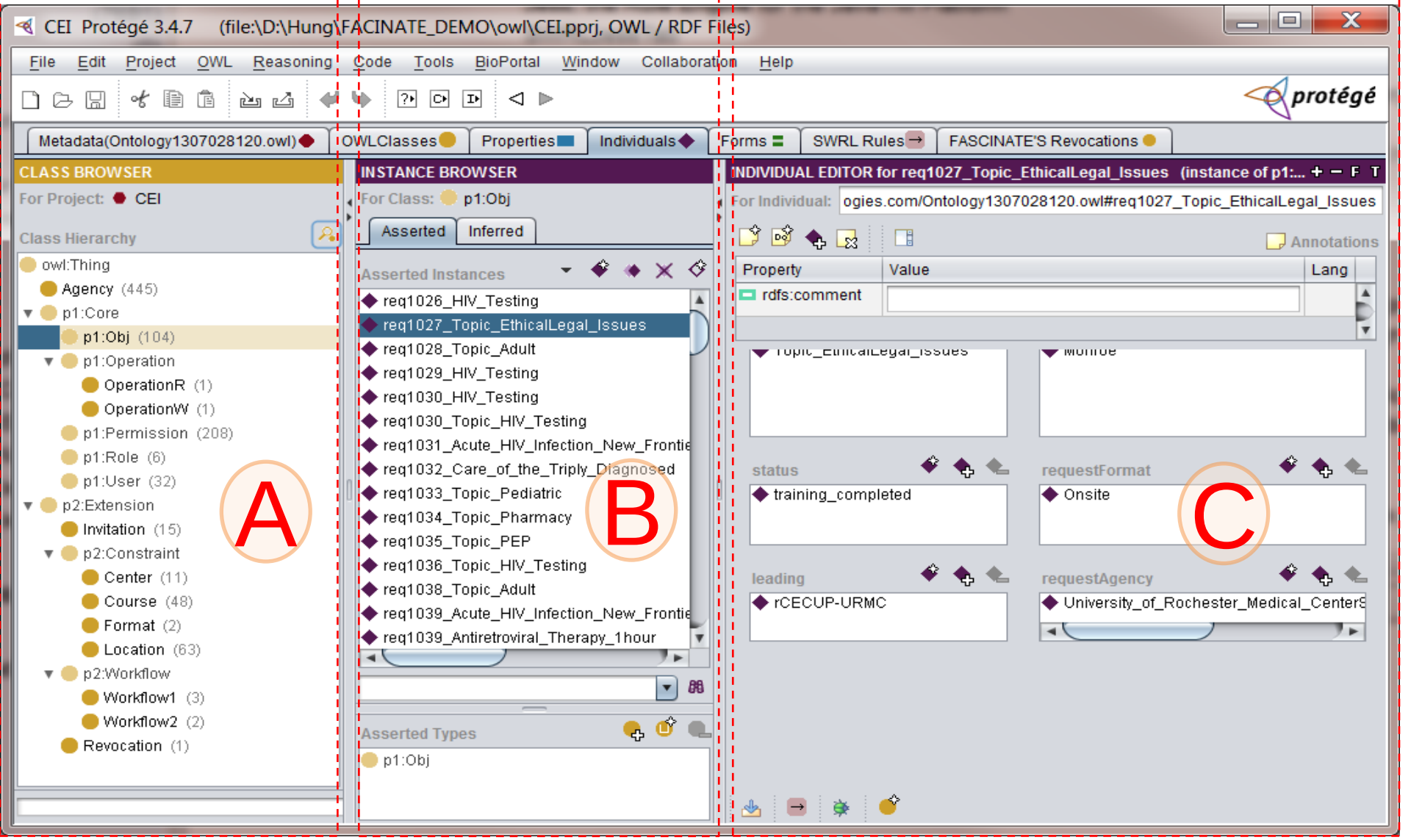


Implementation Framework

A .Protégé Classes:
p1: core RBAC
p2: RBAC Extension

B .Protégé Instances:
access policy instances

C .Protégé Property of Instances:
values of specific variables for access policies



Policy Encoding and Interpretation (2)

$\forall r \in ROLE, \forall req \in REQUEST, \forall w_i \in WORKFLOWSTATUS_I, \forall op_w \in OPERATION_{WRITE}, \forall course \in COURSE, \forall format \in FORMAT, \forall agency \in AGENCY, \forall loc \in LOCATION:$

$role\text{-}permission(r,req,w_i,op_w) \leftarrow$

$status(req,w_i) \wedge$ (1) bridging entity

$request(req,course,format,agency) \wedge$ (2) bridging entity

$location(agency,loc) \wedge$ (3) bridging entity

$inChargeLocation(r,loc) \wedge$ (4) geographical constraints

$inChargeCourse(r,course) \wedge$ (5) topic constraints

$inChargeFormat(r,format)$ (6) format constraints

(a) in first-order predicate logic

```
p1:rolePermission(?r,?p) ←
workflow1(?w) ∧
permissionRequest(?p,?req) ∧
permissionOperation(?p,?op) ∧
permissionStatus(?p,?w) ∧
operationW(?op) ∧
```

```
status(?req,?w) ∧                                   (1)
requestCourse(?req,?course)
    ∧ requestFormat(?req,?format)
    ∧ requestAgency(?req,?agency) ∧                 (2)
agencyLocation(?agency,?loc) ∧                      (3)
inChargeLocation(?r,?loc) ∧                         (4)
inChargeCourse(?r,?course) ∧                        (5)
inChargeFormat(?r,?format)                          (6)
```

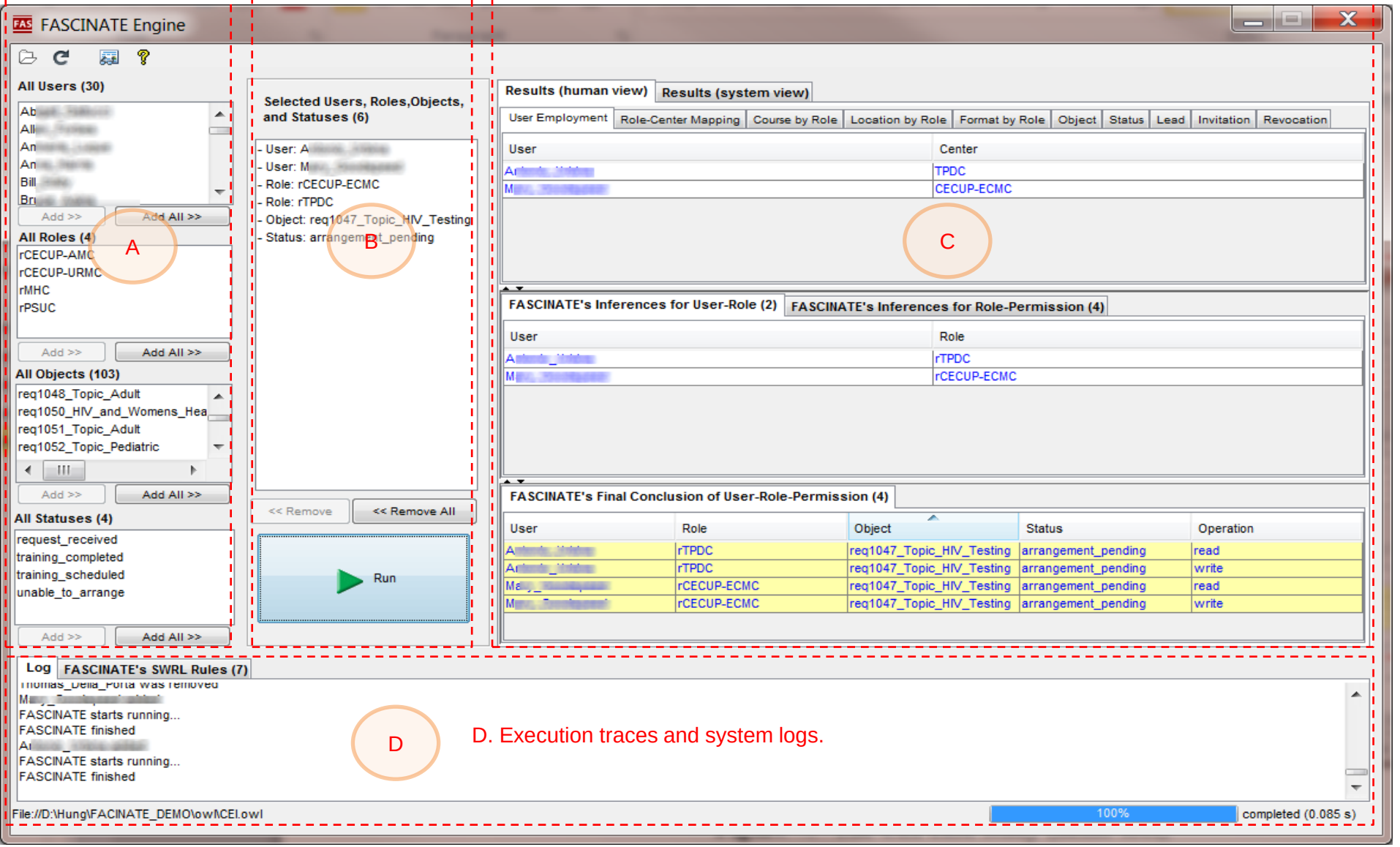
(b) in SWRL

Demo Tool

A.
All users, roles, objects, and workflow statuses

B.
Selected users, roles, objects, and workflow

C.
The results after running the enhanced RBAC on the selected users, roles, objects, and workflow statuses

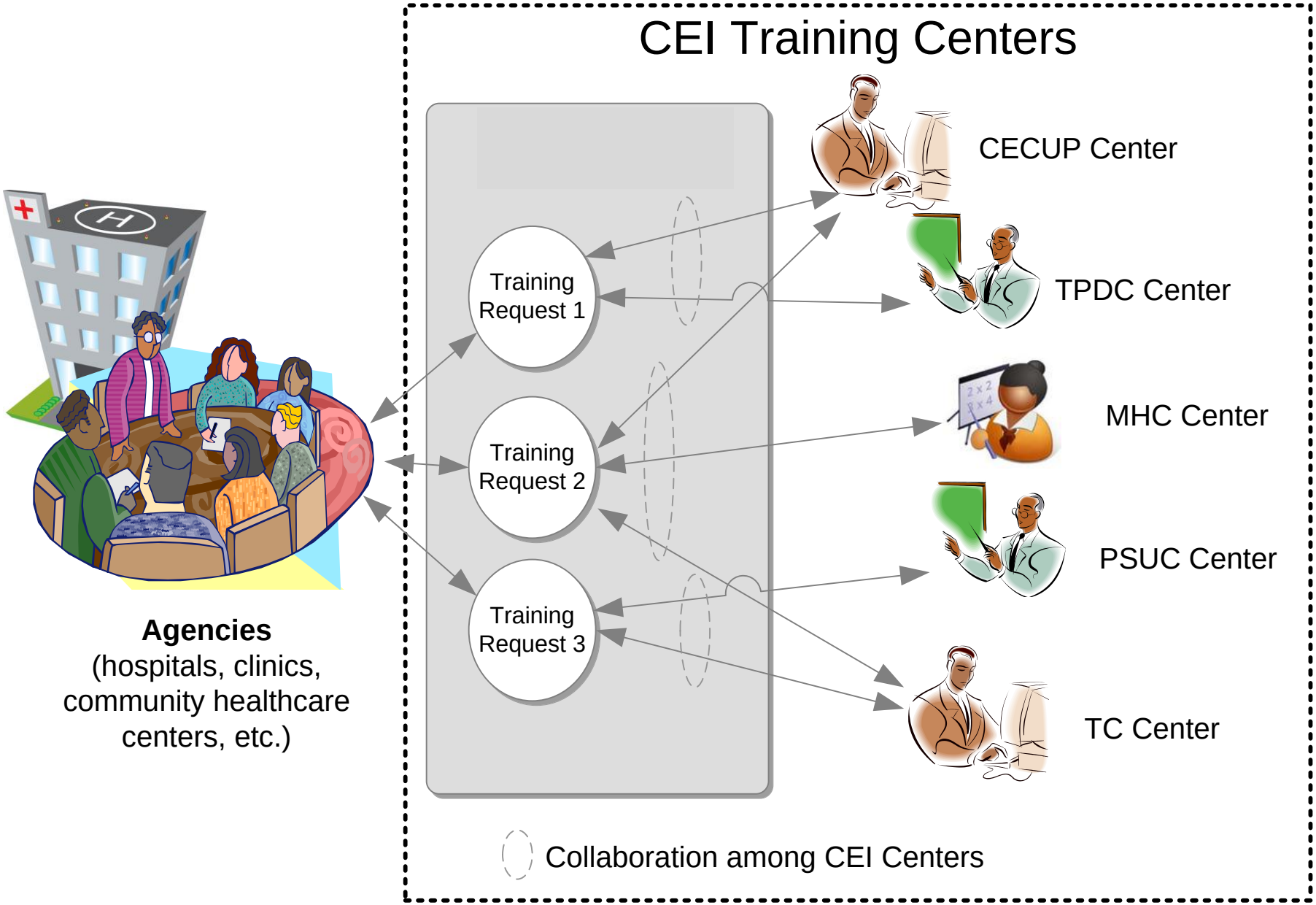


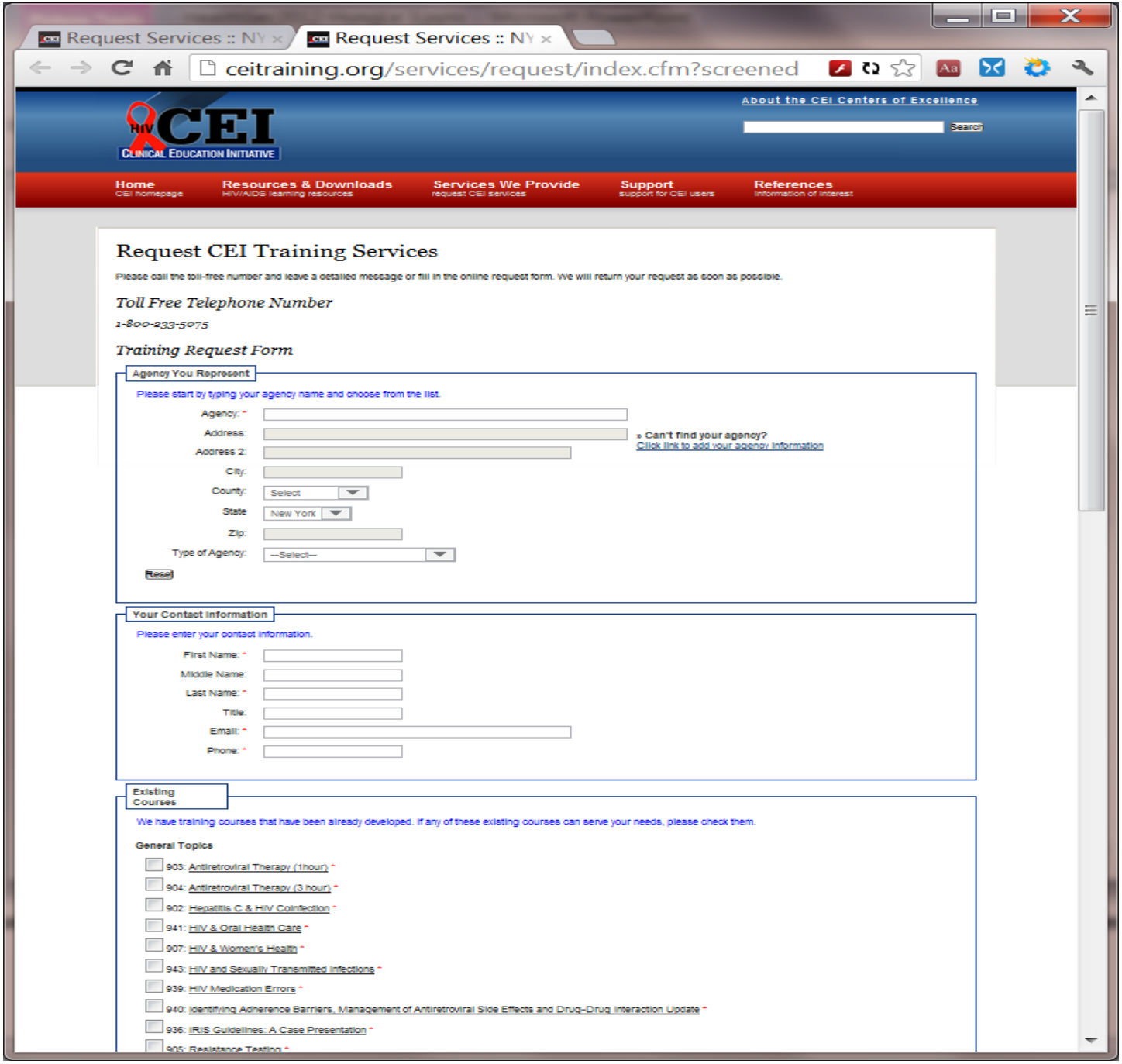
D. Execution traces and system logs.

NYS HIV Clinical Education Initiative (CEI)

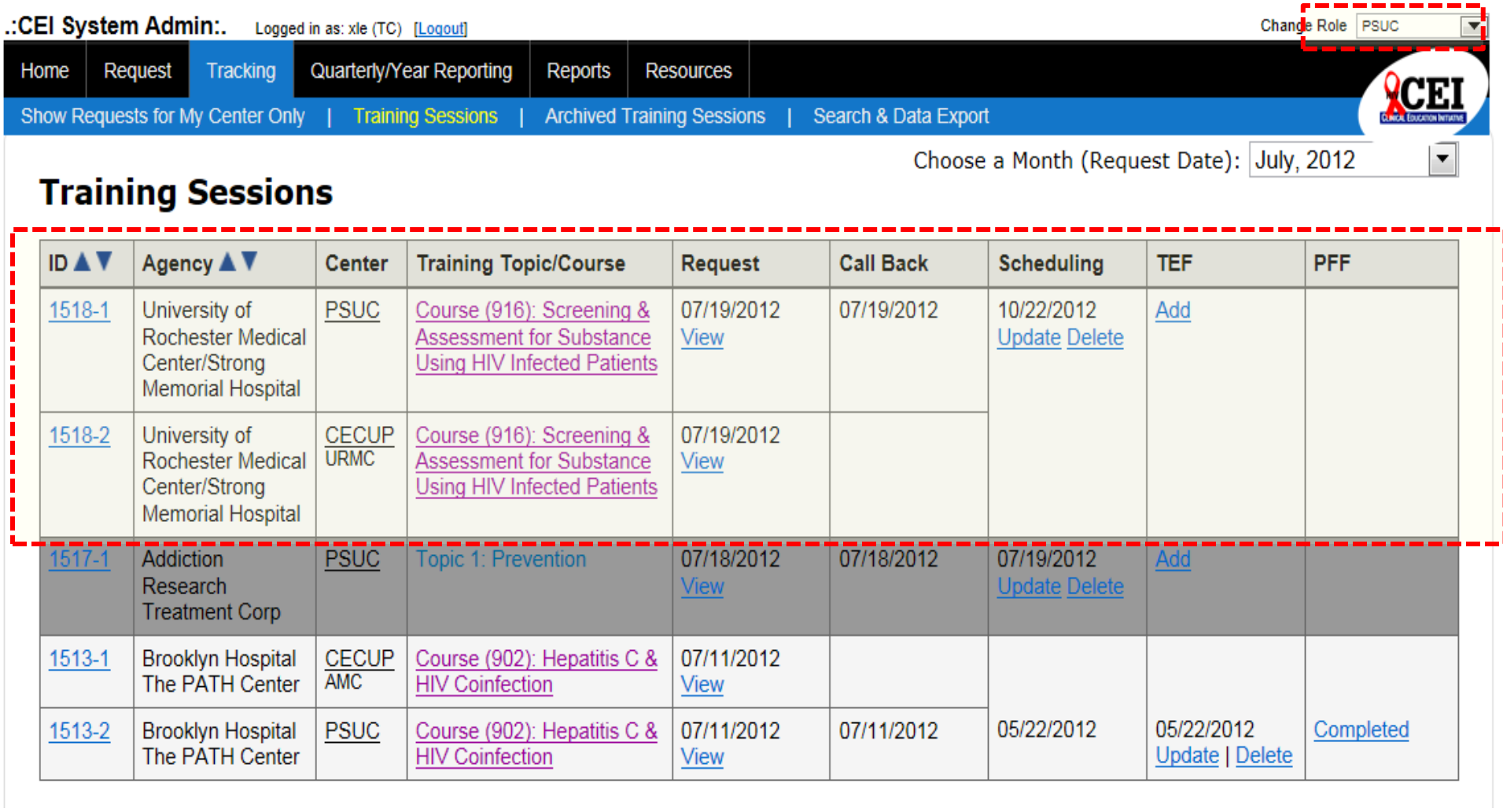
Center	Role	Responsibility	Topic	Location	Format
CECUP	r_{cecup}	onsite training	all topics	upstate region	onsite
TPDC	r_{tpdc}	onsite training	testing, PEP, diagnosis	all areas	onsite
PSUC	r_{psuc}	onsite training	prevention, substance use	all areas	onsite
MHC	r_{mhc}	onsite training	mental health	all areas	onsite
TC	r_{tc}	online training	all topics	all areas	online
RRC	r_{rrc}	resource and referral	all topics	all areas	onsite/online
EC	r_{ec}	evaluation	all topics	all areas	onsite/online

- **CECUP**: Clinical Education Center for Upstate Providers
- **TPDC**: Testing, Post-Exposure Prophylaxis, and Diagnosis Center
- **MHC**: Mental Health Center.
- **PSUC**: Prevention and Substance Use Center
- **TC**: Technology Center

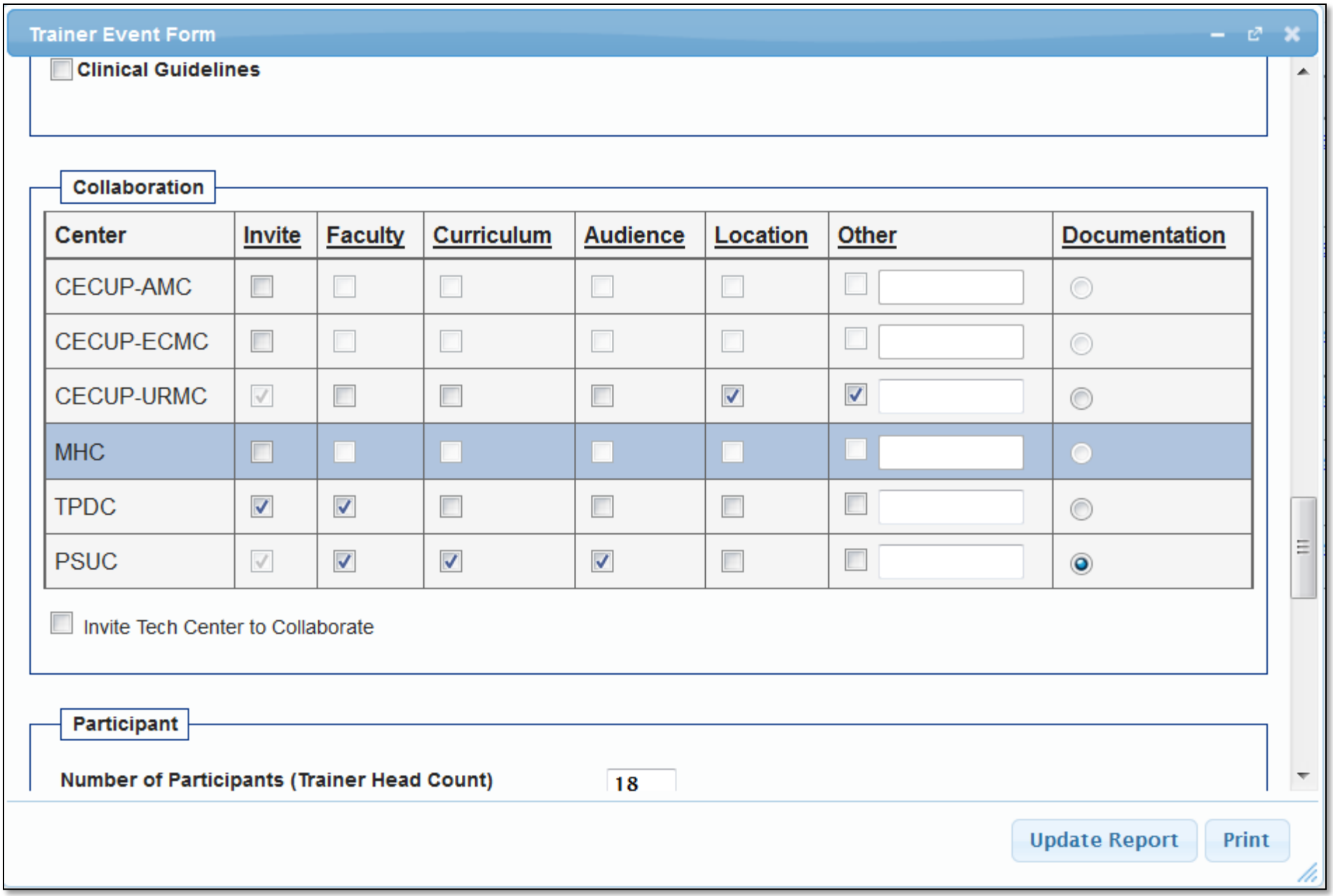

CEI Training Centers
CECUP Center
TPDC Center
MHC Center
PSUC Center
TC Center
Training Request 1
Training Request 2
Training Request 3
Agencies
(hospitals, clinics, community healthcare centers, etc.)
Collaboration among CEI Centers



Online Training Request Form at www.CEItraining.org

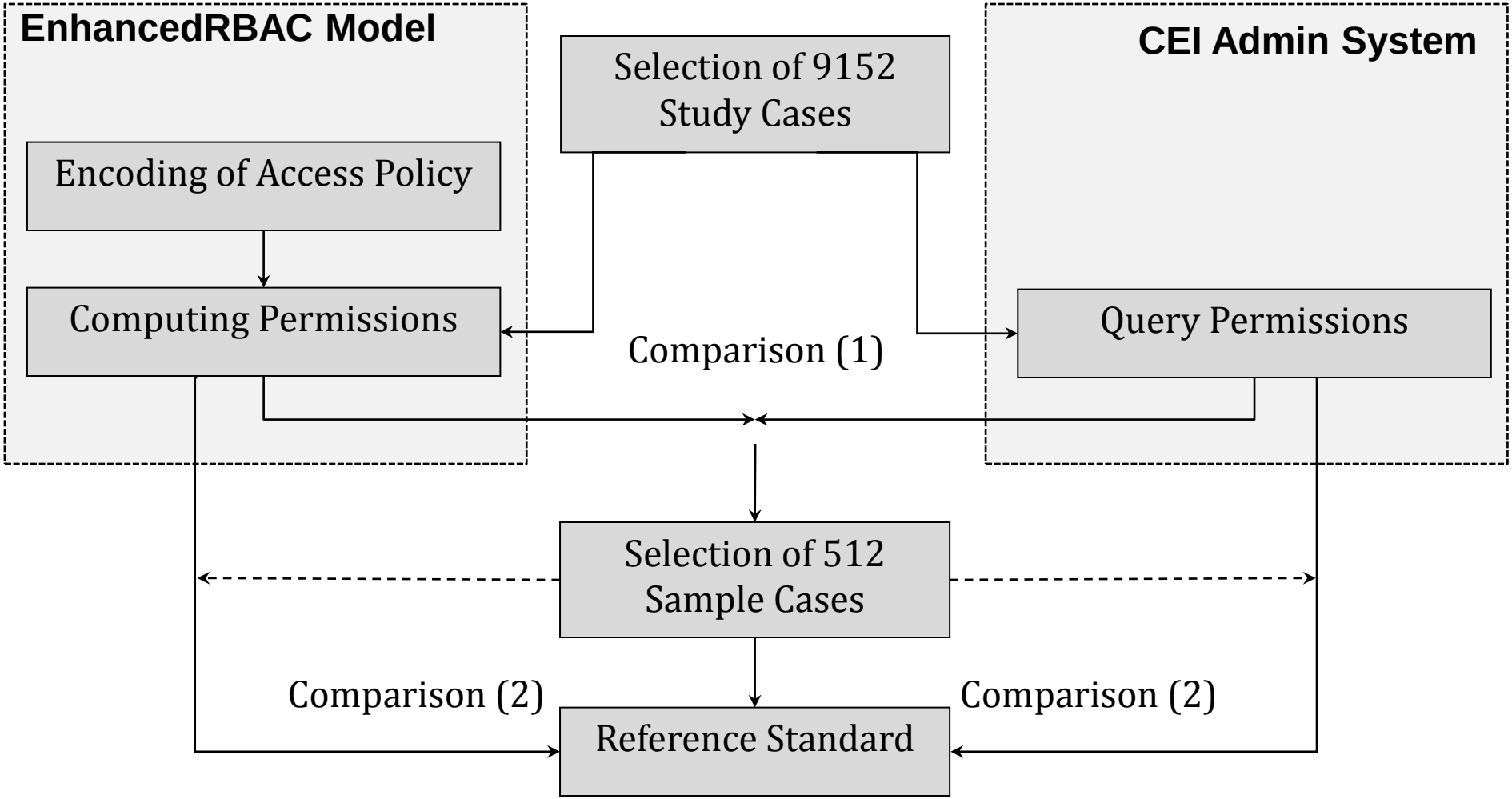


www.CEItraining.org/Admin



Collaboration Form

Evaluation



Evaluation Method

Evaluation (2)

- Highlights of results
  - EnhancedRBAC vs. CEI Admin System
    - Kappa = 0.8-0.89
  - EnhanceRBAC vs. Reference Standard
    - Sensitivity 97-100%
    - Specificity: 100%

Discussion

- First application of access control model for clinical education programs
- Access control is not just restriction of access permissions
- Limitation
- Error analysis
  - Mistakes in preparing invitation data for the study cases to feed EnhancedRBAC
  - Situation to add/delete data directly to/from the CEI Admin database
  - Fault in querying workflow status of the study cases from CEI Admin System

Conclusion

- Successfully developed a system framework to implement the EnhancedRBAC model
- Initial evaluation has shown that this system framework can be effectively used for clinical education
- Future work
  - Extension of this system framework to support the continues development of EnhancedRBAC
  - Deployment of the framework to other domain applications for clinical education, biomedical research, and patient care

Acknowledgement

- The CEI project is sponsored by the New York State Department of Health AIDS Institute.

- Other CEI team members at the University of Rochester Medical Center
  - Dr. Amneris Luque
  - Terry Doll
  - Monica Barbosu
  - Thomas Della Porta

- CEI program staffs
  - Howard Lavigne
  - Dr. Cheryl Smith
  - Lyn Stevens
  - Dr. Bruce Agins
  - and colleagues from other CEI Training Centers for their support.

Thank You !