

Project Description

ACTSI Informatics Architecture Security Infrastructure

Background

The Atlanta Clinical and Translational Science Institute (ACTSI) is funded by the CTSA program (<http://www.ctsaweb.org/>) to promote discovery in clinical and translational research and build novel translational research capabilities. It is a multi-institutional partnership, led by Emory University, Morehouse School of Medicine, and Georgia Institute of Technology, that supports a wide range of studies at collaborating institutions.

The Biomedical Informatics Program (BIP) of the ACTSI has initiated an effort to design and develop an informatics architecture framework and middleware infrastructure, building on existing standards and best practices from the Web, Web Services, Semantic Web, and Grid Computing communities. This effort is driven by use cases and research applications from studies supported by the ACTSI. These studies capture, generate, and reference a variety of datasets stored and managed in multiple systems hosted by different groups and institutions. The ACTSI informatics architecture will support the management, federated query, and integration of databases from ACTSI-supported studies and collaborating institutions, effectively creating a federated ACTSI-wide data warehouse. The federated data warehouse will contain a distributed collection of interoperable databases of various data types, including study specific clinical data, omics data, imaging data (Radiology and microscopy images), tissue specimen information, ECG data, and laboratory data obtained from EMRs.

The databases in the ACTSI federated data warehouse environment may be stored in a variety of database systems and applications. These include caArray, Research PACS, OpenClinica, RedCAP, the Analytical Information Warehouse, microscopy imaging databases, caTissue and Nautilus LIMS, and i2b2. The integration of these systems and federated access to distributed data will be supported by the core components of the ACTSI informatics architecture. These core components provide support in the form of services for ACTSI-compliant data and analytical services, ACTSI-wide identifiers, security, federated query, workflow, and provenance tracking.

Scope of Work

Security is a critical component in the ACTSI environment. The federated ACTSI data warehouse should implement mechanisms for authentication, authorization, trust management, access control, secure information exchange, and auditing. These mechanisms will need to support secure and controlled access to information in a federated environment with services hosted at multiple institutions. Presently the ACTSI informatics architecture effort is considering the caGrid GAARDS infrastructure, NHIN security specifications, and Shibboleth. The GAARDS infrastructure, for example, provides a suite of services, tools, and GUIs for 1) Grid

account management and federation, 2) management of a trust fabric, 3) Grid-wide group management for authorization, and 4) authentication and service-level and service-method-level authorization. The Center for Comprehensive Informatics is in the process of developing a role-based instance and attribute level access control using GAARDS and the Common Security Module (CSM) from the cancer Biomedical Informatics Grid (caBIG) program.

This work request focuses on the design and implementation of tools, techniques, and middleware components that will enable specification and enforcement of data-model-level, data-instance-level, and data-attribute-level access control policies.

Specific tasks to be performed:

- **Task 1:** Develop an attribute-based access control mechanism and associated tools. This mechanism should build on standards, such as XACML, and best practices. It should provide tools for resource providers and clients to use.
- **Task 2:** Evaluate and integrate attribute based access control mechanisms in the ACTSI informatics security architecture. The developed mechanisms should allow specification and enforcement of access control policies in a federated environment. Resource providers should be able to specify access control policies for their resources, and the ACTSI security infrastructure should be able to enforce these policies in federated queries involving multiple resources.
- **Task 3:** Develop extensions to support integration of dynamic policies for authorization and access control.
- **Task 4:** Develop and evaluate techniques for scalability and efficiency of the access control mechanisms. This task could involve the design and development of indexing strategies and information disclosure with redactable signatures.

Requirements:

- The team chosen to carry out this work should develop an initial set of incremental tools that build on and extend the GAARDS and CSM infrastructure and lead to software that is deployable throughout ACTSI after the end of one calendar year. The team is also encouraged to lead an effort to develop a more ambitious security architecture that can be developed and deployed in following years.
- The software, development and testing environment must be openly accessible to all Emory, Morehouse and GaTech ACTSI BIP, BERD and CIN researchers and software developers. **All software developed will be open source under a caBIG style license.** ACTSI will supply the hardware and software development environment if necessary.
- The design of the tools and techniques must be driven by the use cases from the

ACTSI supported studies and those identified by the ACTSI informatics architecture design effort.

- The tools must be compatible with the ACTSI informatics architecture design and the ACTSI informatics middleware infrastructure. The design of the tools and techniques must be done in close working collaboration with the ACTSI informatics architecture team.
- The development team must actively collaborate with the ACTSI informatics architecture working group. All funded participants must attend the weekly working group meeting in person or by phone.
- The all student, postdoc and developer team members must work at least one day at Emory to collaborate with the ACTSI informatics architecture team.