

# SOFA: Service-Oriented Federated Authorization

Andrew Simpson  
(and Paul Jeffreys, David Power and Mark Slaymaker)

Oxford University Computing Laboratory

March 2010

- 1 Motivation and background
- 2 sif
- 3 SOFA
- 4 Applications
- 5 Progress

# Motivation

- Increasingly, there is a drive in many contexts to link distributed data sets
- Often, the distribution of, and responsibility for, such data represents the administrative structures of the organisation
- Typically, there are issues of (systems, syntactic and semantic) heterogeneity to overcome
- And then there are issues pertaining to integration with legacy systems

## An example

- The University of Oxford maintains a centralised, enterprise-level system that monitors the progress of students
- The Undergraduate Admissions Office runs its own database, which is based on the centralised database—with data being transferred periodically
- Some departments run their own admissions databases, which are populated from the centralised admissions database

## An example

- The University of Oxford maintains a centralised, enterprise-level system that monitors the progress of students
- The Undergraduate Admissions Office runs its own database, which is based on the centralised database—with data being transferred periodically
- Some departments run their own admissions databases, which are populated from the admissions database
- And then there is finance, personnel, etc.

## An example

- The University of Oxford maintains a centralised, enterprise-level system that monitors the progress of students
- The Undergraduate Admissions Office runs its own database, which is based on the centralised database—with data being transferred periodically
- Some departments run their own admissions databases, which are populated from the admissions database
- And then there is finance, personnel, etc.
- And that's before we start to think about colleges

## An example

- Of course, all this is perfectly natural in any large organisation
- However, it makes 'joined up' data analysis difficult
- And even if it is possible to integrate disparate systems appropriately, enforcing appropriate and effective access control in the emergent virtual organisation is a significant challenge

- sif (service-oriented interoperability framework): developed within the TSB-funded GIMI (Generic Infrastructure for Medical Informatics) project
- Acts as a combined security and federation layer
- Facilitates the secure sharing and aggregation of data from (more or less) any structured data source
- Based on Java and web services
- Gives rise to a variety of patterns of use

## Patterns of use

- 'Secure' pipelines
- 'Windows' on research data
- Lightweight federation
- Integration of central systems with outliers

# Examples

- Portal for Dementia research data
- Remote, secure access to file stores
- Linking of admissions and student data
- etc.

## Which is all very well, but . . .

There is a dependency on XACML, which is  
*expressive and flexible*

but also  
*verges on the unmanageable*

# SOFA: Service-Oriented Federated Authorization

- In simple terms, the idea is to map sif's approach to integration to issues of authorisation interoperability
- Just as sif's bottom-up philosophy makes no assumptions about technology or data models, nor should it about approaches to authorisation
- It may be that one partner favours access control lists, one utilises RBAC, and one leverages the expressiveness of XACML

## Key deliverables

- An extended version of sif
- A policy construction tool
- Code developed within the project released under a CDDL (Common Development and Distribution License)
- Three systems left in place beyond the end of the project

## What we're not concerned with

- Authentication / federated identity management
- Semantic integration

## Three applications

- University administration (in conjunction with University Administration and Services at the University of Oxford)
- Medical research (in conjunction with the Oxford Biomedical Research Centre)
- Systems biology research (in conjunction with the Oxford Centre for Integrative Systems Biology)

# Progress

- Web site established; management document submitted
- Initial requirements meetings with end-users
- Requirements documents written
- Initial paper submitted
- Lots of coding(!)