

# Role Based Access Control in Web Services based enterprise IT

Peter Gietz, DAASI International GmbH

Heidelberger Innovationsforum, 25.11.2008

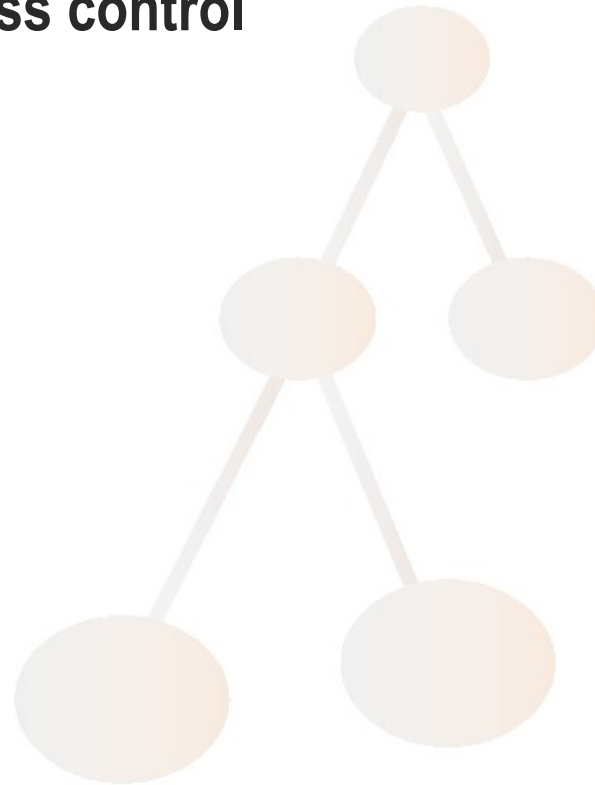
**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Agenda

- Web Services enterprise IT
- Role Based Access control
- OpenRBAC



**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# DAASI International GmbH

- “Directory Applications for Advances Security and Information management“
- Experts in identity management, federations, public key infrastructure, and Grid-Computing
- An Open Source company
- Spin-Off from University of Tübingen
- research oriented, application-driven, competent
- Our aim: user-friendly state-of-the-art products
- [www.daasi.de](http://www.daasi.de)

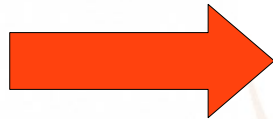
**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Web Services

- Enterprises have „historically grown“ IT landscapes
  - Different non interoperable technologies
  - Boundaries between systems
  - Too little interaction of systems leads to redundancies of data and work processes
  - Work processes often are modelled according to IT requirements and not vice versa



*We need more flexibility!*

- Web Services are seen as the solution to all these problems

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# What are Web Services then?

- **Companies are increasingly recognizing the value of the Enterprise Services Oriented Architecture paradigm**
  - **bridges the gap between business needs and IT delivery**
- **All IT functionality is implemented as independent Web services with enterprise-level business value**
- **Elevates the concept of Web services design, management, and application composition to an enterprise level**
  - **that helps meet business requirements**
- **Thus we have different Systems loosely coupled**
- **They can talk with each other via standardized Protocols**
  - **SOAP, WSDL, UDDI**

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Web Services Standards

## ➤ SOAP

- a framework for exchanging XML-based information in a network
- SOAP used to be an acronym: Simple Object Access Protocol

## ➤ WSDL (Web Service Description Language)

- an XML-based language for describing network services
- WSDL descriptions of capabilities and locations of services
- like an interface description language for Web services
- communication using SOAP or direct HTTP

## ➤ UDDI (Universal Description, Discovery, and Integration)

- provides a registry mechanism for clients and servers to find each other
- uses SOAP for communication

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Role Based Access Control

- **Use of roles to control access**
  - is an effective means for developing and enforcing enterprise-specific security policies
  - helps streamlining the security management process
- **Users are granted membership into roles based on their competencies and responsibilities in the organization**
- **RBAC simplifies the administration and management of privileges (access rights)**
  - roles can be updated without updating the privileges for every user on an individual basis.
  - Users can easily assigned to roles without changing any access rules
  - Users change often, roles don't
- **RBAC also simplifies regulatory compliance**

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Role Based Access Control

- There is an ANSI-Standard for RBAC which includes
  - role hierarchies
    - e.g. role staff member is included in role administrator
    - This again reduces number of access rules
  - Concept of operations
    - unit of control that can be referenced by an individual role
  - Separation of duty
- The Standard defines all needed Methods, e.g.
  - AddUserToRole
  - CheckAccess
  - ...

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# OpenRBAC

- **OpenRBAC is an implementation of the complete ANSI-Standard**
- **Data are stored in an LDAP directory**
  - **For fast read access**
  - **For best integration into existing user management systems**
- **Around this core implementation there is a Web Service Layer**
  - **Access Control can be centrally managed within a Service Oriented Architecture**
  - **Web Services are resources as well as Data, Storage, etc. They all can be controlled by the central RBAC system**
  - **In addition to the Methods defined in the standard new methods have been developed as Web Services**

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# OpenRBAC

- **OpenRBAC**
  - is Open Source Software
  - Is compliant to international standards
  - Is available at [www.openrbac.org](http://www.openrbac.org)
  - has been further developed and deployed within research projects on Grid-Computing (D-Grid initiative [www.dgrid.de](http://www.dgrid.de))
  - Can flexibly be enhanced to fulfil additional requirements
  - Can help enterprises in controlling resources within service oriented infrastructures
- **We are currently looking for enterprise partners for pilot projects**

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Pilot project example

- Analyse access control requirements
  - Including regulatory compliance
- Develop a role model for the enterprise
- Deploy OpenRBAC
- Integrate OpenRBAC into existing Web Services
- Report the benefits of the pilot system
- Plan a production system

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Thanks for your attention

➤ Any Questions?

➤ Please ask me:

- Peter Gietz, DAASI International GmbH
- [www.daasi.de](http://www.daasi.de)
- [peter.gietz@daasi.de](mailto:peter.gietz@daasi.de)

**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management

