



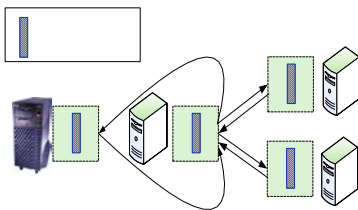
# THE WHITE ROSE GRID e-Science Centre

## Instance-Level Security Management in Web service Business Processes

### Introduction

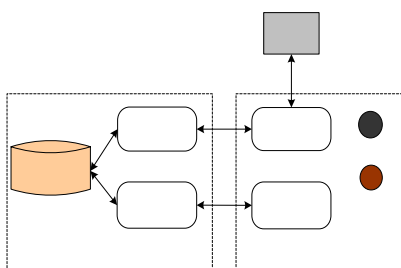
In this research, we investigate the security issues related to instances of Web services business processes (i.e., business session), and demonstrate that security mechanisms are needed at the instance level to help session partners generate a reasonable trust relationship. To achieve this objective, an proposed. Experimental systems are integrated with both the GT4 and CROWN Grid infrastructures, and comprehensive experimentation is conducted to evaluate our authentication mechanism.

Additionally, we design a policy-based authorization mechanism which allows an instance invoker to dynamically assign fine-grained access control policies for the new invoked instance so as to grant other session partners the necessary permissions.



### Multi-party Authentication for Web service Instance

Our authentication system attempts to directly authenticate service instances rather than users, which is different from the conventional authentication systems mentioned above. In our authentication system, every instance is associated with a pair of keys. The public key is used as the identifier of the instance, while the private key is kept secretly and used to prove the possession of the identifier. All the identifiers of the session partners and other related information of a business session are stored in a Session Authority, SA. When a new service instance is invoked by a business session, the identifier and other related information will be sent to the SA so as to guarantee the validity of the



information kept by the SA.

### Experiments

These experimental systems are mainly used to evaluate the scalability and the performance of our instance-level authentication system. In some experiments, our authentication system can execute stably until over 260,000 instances are generated. Such experimental results demonstrate the scalability of the instance-level authentication system is good. Additionally, compared with the performance of service-level security mechanisms, the overhead introduced by our instance-level authentication system is reasonable.

### An Instance-level Authorization Mechanism

Web service business processes rely on the peer-to-peer interactions between participant instances. Sometimes the invoker needs to assign its own access control policy to this new invoked instance. In order to address this issue, we propose an instance-level authorization mechanism which is designed for Web service business processes. In our system, the invoker can dynamically specify the access control policies of the invoked instance at run-time, and thus the access control relationship between instances is more flexible. Additionally, with the assistance of the instance-level authentication system, our mechanism can define the business session constraints within the access control policies.

### Further Information

Contact: Dacheng Zhang  
email: [dcz@comp.leeds.ac.uk](mailto:dcz@comp.leeds.ac.uk)

