National e-Science Centre

Tutorial 3: Globus Development

John Watt, National e-Science Centre

Tutorials Timetable

National e-Science Centre

Week	Day/Time	Topic	Staff
3	Fri 11am	Introduction to Globus	J.W.
4	Fri 11am	Globus Development	J.W.
5	**Fri 11am**	**Globus Development**	**J.W.**
6	Fri 11am	Condor	J.W.
7	Tue 12pm	SAML/PERMIS (L)	A.S.
7	Wed 12pm	Portals (L)	J.J.
7	Fri 11am	Q & A Session	all
8	Fri 11am	OGSA-DAI (L)	O.A.
10	Tue 12pm	Example Systems (L)	R.S.
10	Fri 11am	Assignment Demos	all

Recap

National e-Science Centre

- **Last time we:**
  - Described the composition of the container
  - Mentioned the usefulness of ‘stubs’
  - Examined the generic security infrastructure
    - Certificates, grid-mapfile
  - Looked at the components of a WSDL file
  - Described the content of the deployment descriptor

- **This week we’ll look at implementation files, building and deployment, then some advanced security**
  - And then mark your Problem Set 3!

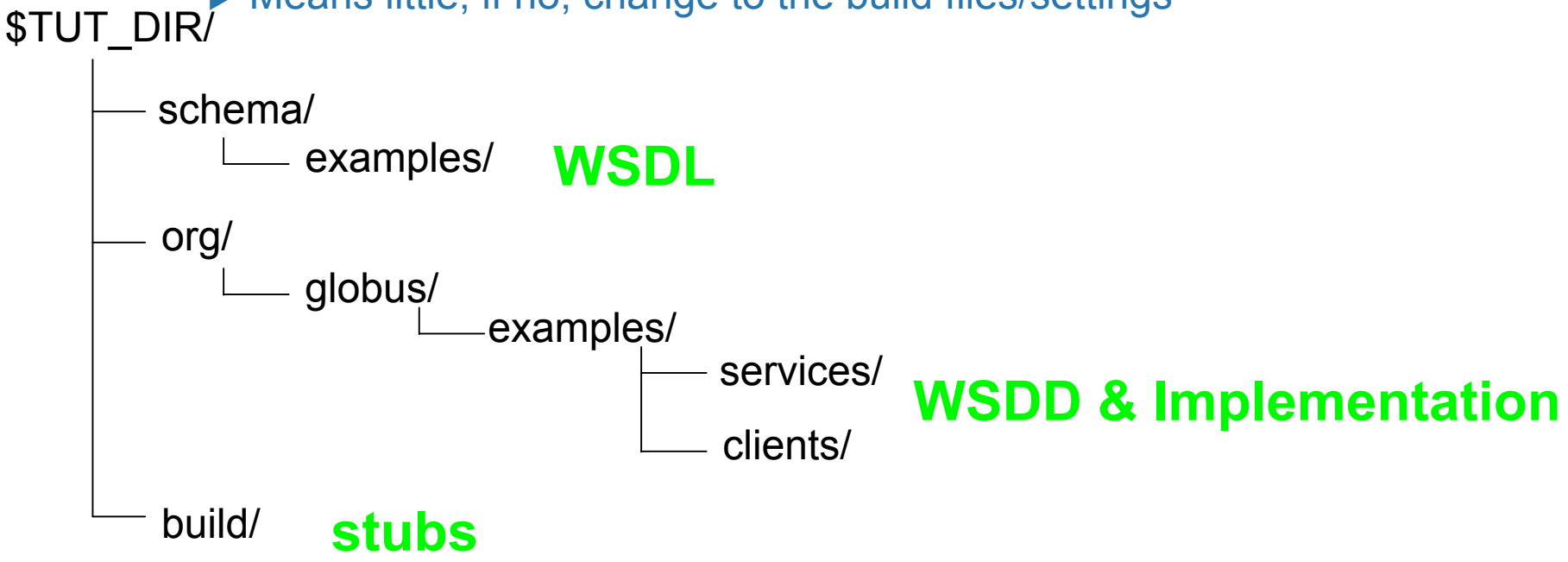
Exercise

- **Did anyone try comparing a proxy certificate and a user certificate?**
  - **Two major points to notice:**
    - The Subject DN of the proxy certificate is different from your original user certificate
      - It has an extra random number appended to it
    - More importantly, the ISSUER of your proxy certificate is not the Certificate Authority, but it is YOUR ORIGINAL CERTIFICATE
      - Actual proxy certificate holds three pieces of info
        - » Your Short-lived proxy certificate
        - » The proxy certificate's private key
        - » The original certificate (acting as a root CA)
      - Proxy's private key can sign more copies of the proxy, hence propagate your identity round the Grid…

Directory Structure

National e-Science Centre

- **Correct directory structure is essential**
  - **We recommend you stick with the generic structure**
    - Means little, if no, change to the build files/settings



Qnames

- **Yet another bespoke mappings file…**
  - This lives in the same directory as your implementation file
  - Provides a syntax for Java to refer to almost any aspect of your service
  - Joins the service namespace and Resource Property into one statement
  - QName for the ‘last_action’ Resource Property (from last week) would be:
    - {http://www.globus.org/namespaces/Our_Service}last_action

Implementation file

- Service.java file
- Headers
  - Define your package

```
package org.globus.services.OurService.impl
```

  - Grab the Java Remote Exception library

```
import java.rmi.RemoteException
```

  - Import standard Resource Property libraries

```
import org.globus.wsrf.ResourceProperties
```
etc…

  - Import the service message stub files that Ant created

```
import org.globus.services.stubs.OurService
```
etc…

Implementation File

- Java implementation code goes next

```
public class OurService implements Resource,
   Resource Properties {
}
```

  - Service implements service operation and resource (stateful part)
  - Require definitions of our WSDL Resource Properties

```
private String do_it
private String last_action
```

  - Then implement the operations (app. dependent)

Security

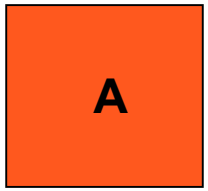
National e-Science Centre

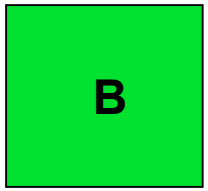
- **Implemented by the Grid Security Infrastructure (GSI)**
  - **Based on Public Key Cryptography**
  - **We have seen our credentials in the form of X.509 Digital Certificates**
  - **We have seen PROXY certificates created from these credentials**
    - Proxies implement DELEGATION
    - This allows your job to run on multiple resources without having to read your private key each time

Mutual Authentication

National e-Science Centre

- Two sites A and B wish to identify each other

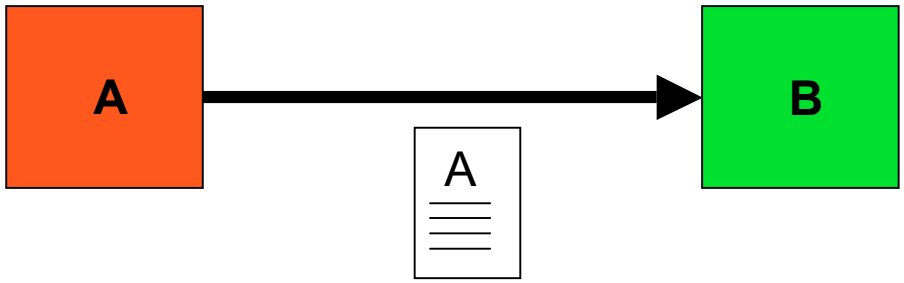




Mutual Authentication

National e-Science Centre

- **Two sites A and B wish to identify each other**

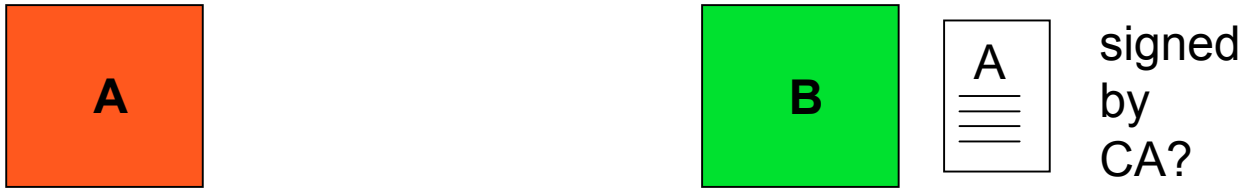


• A gives B their certificate

Mutual Authentication

National e-Science Centre

- **Two sites A and B wish to identify each other**

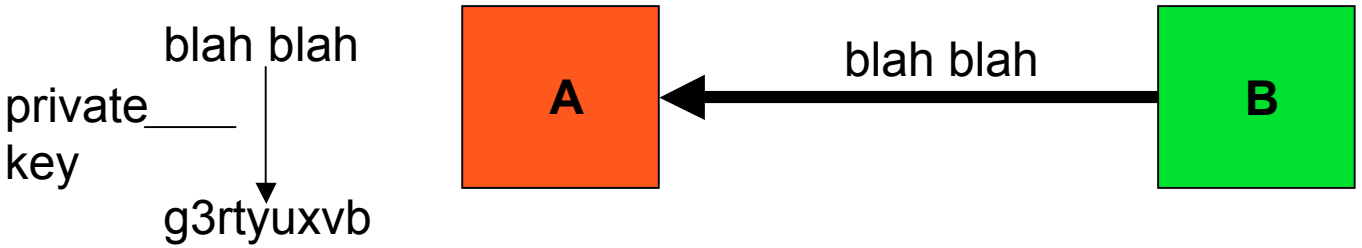


- A gives B their certificate
- B checks that a trusted CA signed the certificate

Mutual Authentication

National e-Science Centre

- **Two sites A and B wish to identify each other**

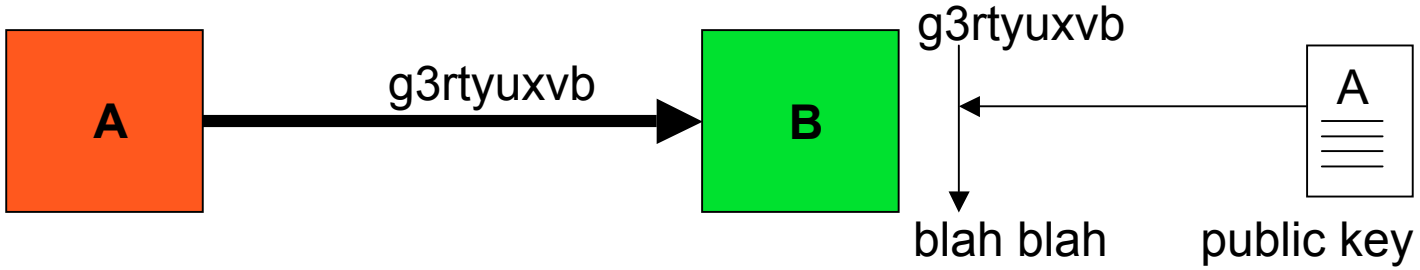


- A gives B their certificate
- B checks that a trusted CA signed the certificate
- B sends A a message to encrypt using A's private key

Mutual Authentication

National e-Science Centre

- **Two sites A and B wish to identify each other**

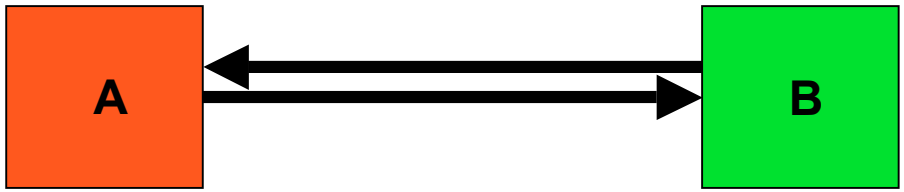


- A gives B their certificate
- B checks that a trusted CA signed the certificate
- B sends A a message to encrypt using A's private key
- A sends encrypted message back to B, B decrypts using A's public key

Mutual Authentication

National e-Science Centre

- **Two sites A and B wish to identify each other**



- A gives B their certificate
- B checks that a trusted CA signed the certificate
- B sends A a message to encrypt using A's private key
- A sends encrypted message back to B, B decrypts using A's public key
- If original message is retrieved, A and B are "mutually authenticated"

Types of Security

National e-Science Centre

- **Remember our –nosec flag?**
  - **This tells the container not to implement TRANSPORT security for its services**
- **What does this mean?**
  - **GT4 can implement TRANSPORT and MESSAGE level security**
  - **In general,**
    - TRANSPORT
      - Everything in the HTTP transfer is encrypted/signed
    - MESSAGE
      - The message contained within the SOAP envelope is encrypted/signed

Types of Security

National e-Science Centre

- GSISecureMessage
  - Based on WS-Security standard, good for few messages
- GSISecureConversation
  - Based on WS-SecureConversation spec., good for many messages
  - Allows credential delegation (proxies)
- GSITransport
  - Based on TLS/SSL
  - Most secure, but doesn't support delegation

Types of Security

National e-Science Centre

- All the above schemes are not mutually exclusive
  - A mixed bag…
- All support encryption and signature checking
  - ENCRYPTION
    - Guarantees PRIVACY
    - contents cannot be viewed by external agents
  - SIGNATURE
    - Guarantees INTEGRITY
    - Contents have not been manipulated by external agents

Securing a Service

National e-Science Centre

- **Service requires a security descriptor**
  - **No change needed to any of your implementation**
    - Although some services add security logging to facilitate useful debugging

```
<securityConfig xmlns="http://www.globus.org">
        <authz value="none“/>
</securityConfig>
```

  - **This tells any services referencing this security descriptor that we don’t want any authorisation done**
    - Options include: custom, grid-map, VOMS

Securing a Service

National e-Science Centre

- The only change we need to make is in the service deployment descriptor (WSDD)

```
<parameter name="securityDescriptor"
  value="etc/org_globus_services_security_Ou
  rService/security-config-OurService.xml"/>
```

- This line tells the service to reference the security descriptor
  - Note that because the security descriptor doesn't say what kind of security mechanism it supports, the client is free to choose how it connects

A Secure Client

National e-Science Centre

- We only need to add two lines to our client

```
((Stub)math)._setProperty(Constants.GSI_SEC
  _CONV,Constants.ENCRYPTION);
((Stub)math)._setProperty(Constants.AUTHORI
  ZATION,NoAuthorization.getInstance());
```

  - Here we are asking to use GSISecureConversation using encryption and No CLIENT-SIDE Authorisation

Hints and Tips

National e-Science Centre

- **We DON'T recommend writing everything from the start**
  - **Better to take an existing service and substitute your service names etc..**
  - **WATCH THE DIRECTORIES**
    - Most problems come from
      - Stubs not being pointed at properly
      - Missing import links
- **Copy a version of helloworld/tutorial so you can start from scratch again if you get lost**
- **Always deploy your service as 'globus'**
  - **If not you can end up with some directory permission problems that prevent deployment**
- **NO transport security is needed**
  - **Local containers should run with -nosec**

Useful Links

National e-Science Centre

- GT4 Tutorial *(The Sacred Text!)*
  - http://gdp.globus.org/gt4-tutorial
  - Locally: $HOME/progtutorial.pdf

- GT4 Components
  - http://www-unix.globus.org/toolkit/GT4Facts/
- National Grid Service
  - http://www.grid-support.ac.uk/
  - You are already registered in their grid-mapfile…

National e-Science Centre

Problem Set 3 Assessment

Next Week… Condor