Enabling Grids for
E-science in Europe

www.eu-egee.org

Exercise 7

GT3 Security: Share Files Securely

GT3 Security Details

Enabling Grids for E-science in Europe

- Built on top of PKI
  - Each entity has two keys: public and private
  - Data encrypted with one key can only be decrypted with other
  - The private key is known only to the entity
- The public key is given to the world encapsulated in a X.509 certificate

Certificates

Enabling Grids for E-science in Europe

- A X.509 certificate binds a public key to a name
- It includes a name and a public key bundled together and signed by a trusted party (Certificate Authority)
- An example of a Distinguished Name (DN):

  “/O=Tutorial/OU=User/CN=Charles Bacon”

Certificate Authorities

Enabling Grids for E-science in Europe

- A Certificate Authority (CA) signs certificate requests
- To verify a certificate signature, you must have a copy of the CA certificate
- By default, stored in /etc/grid-security/certificates
- For our tutorial, stored in $TUTORIAL_LOCATION/certificates

Proxy Certificates

Enabling Grids for E-science in Europe

- Proxy certificates contain a new keypair, and are signed by the original certificate
  - Also has shorter lifetime
  - Stored in /tmp/x509up_u$UID
  - Protected by filesystem permissions
- Create a proxy using org.globus.tools.ProxyInit
  - Full GT3 install includes C command line clients as well

Service-side Authentication

Enabling Grids for E-science in Europe

- XML configuration files designed to set security parameters for a service
- Allows per-method authentication settings
- auth-method
  - none: no authentication
  - pkey: GSI Secure Message
  - gsi: GSI Secure Conversation
- run-as
  - caller: Execute method with caller's credential
  - system: Execute method with container credential
  - service: Execute method with service credential
- Need to mention the XML configuration file in the wsdd as securityConfig parameter

Client-side Authentication

- Can set authentication properties programmatically
- For example, our GetFile client will set GSI Secure Conversation authentication
  - ((Stub)portType)._setProperty(Constants.GSI_SEC_CONV, Constants.ENCRYPTION);

Authorization

Enabling Grids for E-science in Europe

- GT3 allows for different authorization methods
  - Client
    - None: no authorization will be performed
    - Self: service will be authorized if it has the same identity as the client
    - Host: service will be authorized if the host returns an identity containing the hostname
  - Server
    - None: no authorization will be performed
    - Self: client will be authorized if it has the same identity as the service
    - Gridmap: User will be authorized as identity listed in gridmap

Gridmap Files

- A mapping from certificate subject names to local resource identities
  - “/O=Tutorial/OU=User/CN=Charles Bacon” bacon
- Used in the gridmap authorization methods
- Each service may have its own gridmap, specified by the gridmap parameter
- Allows per-site authorization
  - Decentralized control required for VOs

What Attendees Should Do

Enabling Grids for E-science in Europe

- Uncomment the securityConfig parameter in WSDD
- Uncomment the security code in GetFile.java
- Try to GetFile from your service
- Try querying the SDEs of your service
- Create a proxy, then try both again

What Attendees Should See

Enabling Grids for E-science in Europe

- Without a proxy, you cannot interact with your service
- With a proxy, both operations are successful

Exercise 7 Review

Enabling Grids for E-science in Europe

- Service security is configured through parameters in the WSDD file, and in the securityConfig XML file
- Client security is configured by setting properties in the Java code
- Service-side authentication may be specified on a per-operation basis