SIMDAT Industrial Grid Profile Analysis

Mike Boniface	IT Innovation
Hans–Christian Hoppe	Intel

Enterprise Grid Requirements Research Group,
OGF20, Manchester, May 9, 2007

SIMDAT

Information Society
Technologies

Motivation

- ***Understand*** issues with key Grid specs applied to industrial and business applications
  - security, operational, performance requirements
- ***Recommend*** how the specifications can be safely adopted
- ***Publish*** industrial Grid profiles to wider community
- ***Engage*** with appropriate standards initiatives to influence future direction of specs

Specifications and Profiles

- **WS-Addressing (WS-A)**
  - describes the encapsulation and use of a (possibly contextualised) Web Service address via End Point References (EPR)
- **Web Service Resource Framework (WSRF)**
  - collection of specifications, which describes a particular use of WS-Addressing to access resources via contextualised Web Services
- **WS-Notification (WSN)**
  - collection of specifications, which builds further on WSRF to define patterns for transmitting notifications between Web Services
- **OGSA WSRF basic profile**
  - defines normative functionality expected of an OGSA-compliant Grid, building on WSRF and WSN

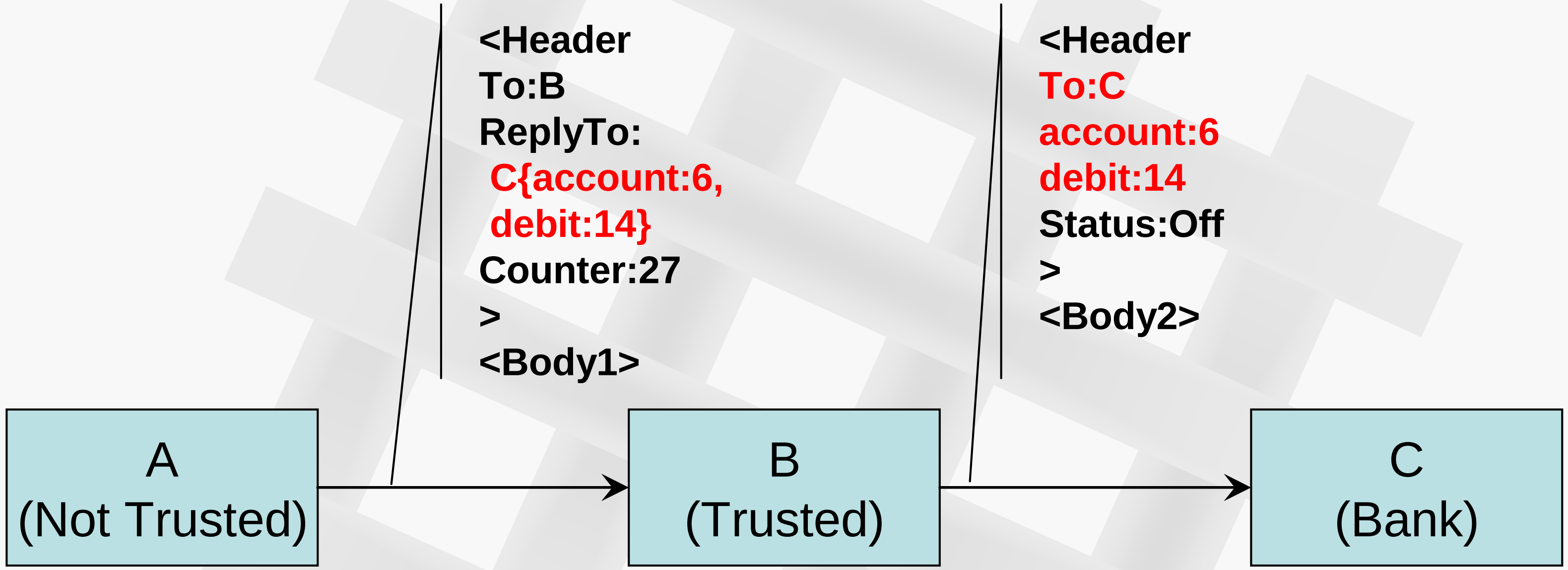
Industrial/Business Scenario Characteristics

- **Dynamic, flexible customer/provider relationships**
  - third parties and intermediaries
  - must have interoperability between providers

- **Security & Trust**
  - different levels of trust between different partners
  - protect information that is important to each partner’s business

- **Operation**
  - definition and effective control of access privileges
  - protect infrastructure against attacks (intrusion, DOS)WS-Addressing (WS-A)

Topic 1: EPRs in WS-Addressing



- B is forced to pass on header elements defined by A
- C cannot tell whether A or B inserted header elements

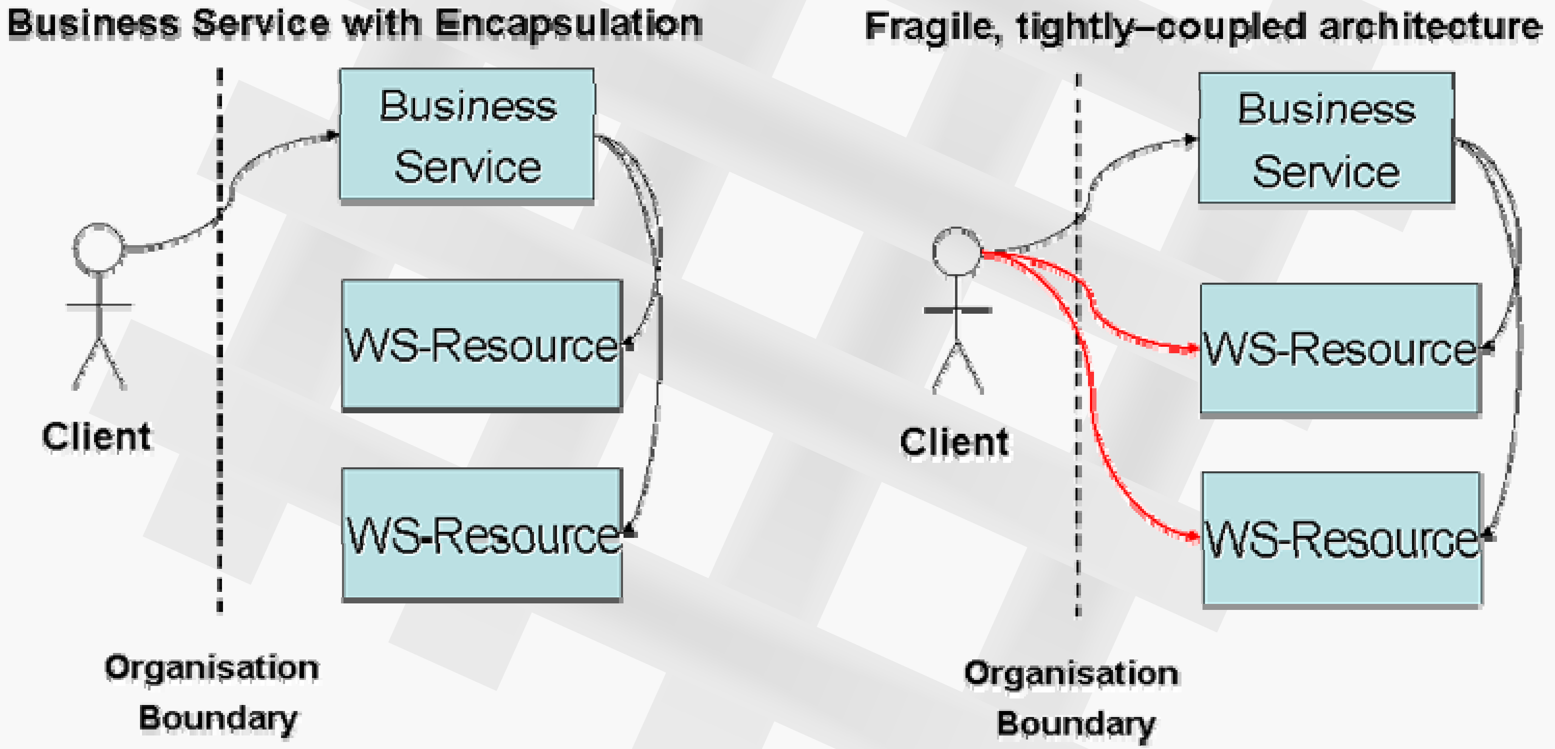
WS-Addressing Options

- Fixes to this problem have been proposed
  - WS-Addressing (Aug ’05 spec) recommendation allows receivers to drop EPRs, marks passed-on header elements ⇒ interoperability problems if header elements are silently dropped, can smuggle in header elements in addresses
  - signing of “genuine” header elements ⇒ multiple signatures in a message

- Our recommendation
  - recipients can constrain where a response generated from an EPR can be sent (e.g. only back to the original sender)
  - OR recipients can constrain which reference parameters or HTTP arguments from an EPR they are willing to handle, e.g. by using a blacklist or whitelist

Topic 2: WS–ResourceProperties

- Breaks normal encapsulation patterns used in successful E–Commerce systems (like http://java.sun.com/blueprints/corej2eepatterns)



Further Issues with WS-ResourceProperties

- Transactional behaviour not defined
  - concurrent access not excluded for set operations
- Access control policies difficult to enforce
  - must understand the semantics and representation of properties
  - must understand any query languages used to retrieve them e.g. XPATH

Options for “Fixing” WS-ResourceProperties

Encapsulation

- the resource property in question is defined by a stable and widely adopted Web Service specification
- OR the request comes from an application that is maintained together with the WS-Resource

Access Control

- specify that the “conversational” resources can have no resource properties, so that all the methods return faults in all cases
- OR allow access to the mandatory GetResourceProperty method of WS-ResourceProperties only, with a fixed set of “well-known” properties and access policies for each WS-Resource
- OR restrict access to WS-ResourceProperties to the host provider of the WS-Resource, thus containing any interoperability problems

Topic 3: WS-Notification Issues

- Family of specifications to support notifications between web services
  - WS-BaseNotification
  - WS-BrokeredNotification
  - WS-Topics
- Supports push and pull style notification
  - so firewall issues are covered ☺
- Access control policies difficult to enforce
  - must understand the semantics and representation of subscriptions
  - information revealed in notifications depends on complex filters
  - destination may not be acceptable to the NotificationProducer, even if the Subscriber were accepted
- Denial-of-Service attacks possible by subscribing on others behalf
- Specification seems to be have written to support situations without resource properties

Call to Arms – Define Industrial Grid Profile

- Objective
  - based on WS-Adressing and WSRF, define a profile that addresses the issues discussed
  - three levels of compliance to WSRF

- Basic WSRF compliance – this is what SIMDAT uses!
  - adopt WS–Adressing, define minimal whitelist for EPR
  - adopt WS–Resource, have a single context ID for all services
  - implement GetResourceProperty, but don't have resource properties declared
  - define BaseFault that is returned whenever users attempt to access a ResourceID for which they are not authorized, or which does not exist

- Extended WSRF/WSN conformance
  - above, plus
  - have set of commonly understood resource properties, accessible only to clients hosted by the same
    provider
  - WS–ServiceGroup should NOT be implemented
  - WS–BaseNotification, WS-BrokeredNotification and WS-Topics to be used in restricted ways: use Notify messages format, subscriptions supported only for parties with the same service provider, publisher registration only with brokers with the same service provider

Call to Arms – Define Industrial Grid Profile

- Full OGSA WSRF Basic Profile conformance – lots of questions
  - if we deny all access to all WS-ResourceProperties operations, or restrict access only to the service provider of each WS-Resource, which features of the OGSA WSRF Basic Profile can be implemented?
  - if we restrict access to GetResourceProperty only, then a single Qname would be the query argument in each request, and the set of available resource properties will be fixed. Could we support authorisation policies easily in that case? If so, how much OGSA functionality could be implemented securely with this restriction in place?
  - can we identify a fixed set of non-sensitive resource properties and notification topics that is sufficient to implement OGSA? If so, does it make sense to specify a profile that only uses these? Does this make sense if we assume that any other resource properties or topics are inaccessible to any but the service provider?
  - if we allow free access to all WS-ResourceProperties operations, which OGSA WSRF Basic Profile features would become dangerous or unacceptable to industrial users?
  - given any reasonable security policy with respect to resource properties, can we infer the security policy that should apply to WSN components and topics required by OGSA?

Read all the Details

- at http://www.gria.org/white_papers.php

OR

- at http://www.simdat.eu