



CITY UNIVERSITY
LONDON



Taming the Cloud

*Safety, Certification and
Compliance of
Software Services*

Howard Foster
Department of Computing

WESOA 2011, Paphos, Cyprus

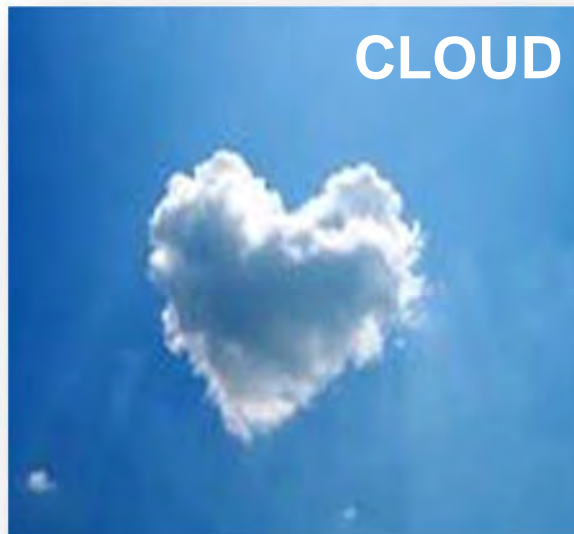




CITY UNIVERSITY
LONDON

Theme

Engineering Service-Oriented Applications ...





CITY UNIVERSITY
LONDON

Cloud in a Box



Linthicum 2009





Cloud Features

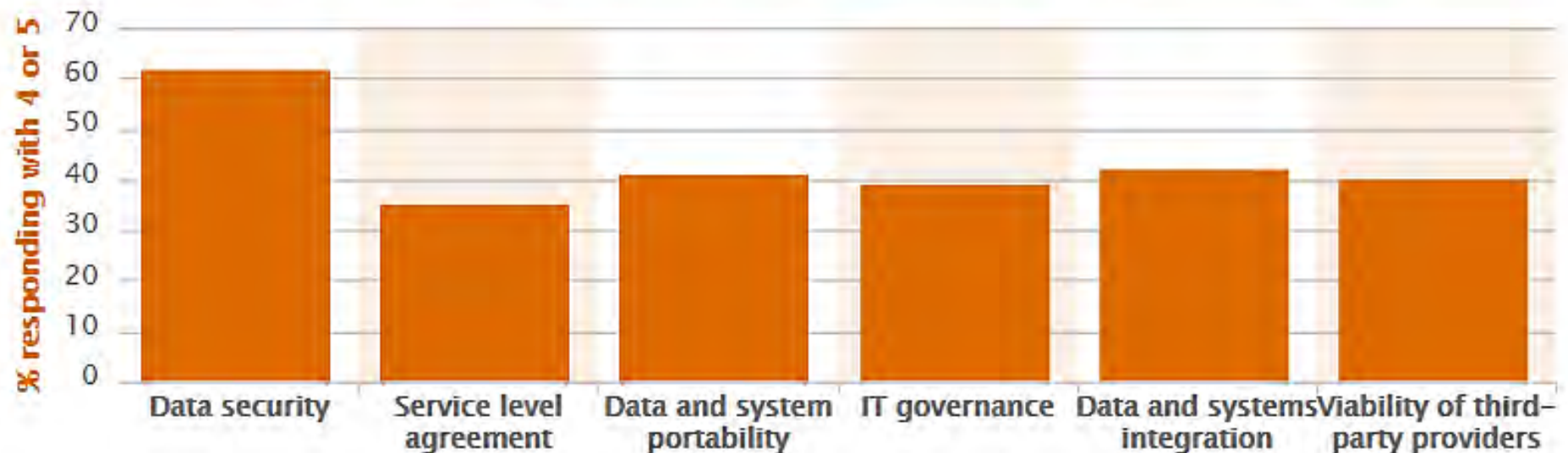
	Benefits	Concerns
Cost	Capital Expenditure moves to Operational (pay-per-use)	Cost up front to re-engineer legacy apps? Moving cloud provider?
Agility	Rapidly re-provision technical infrastructure resources	Rigor, Compliance and <i>potential</i> Loss of Control
Multi-tenancy	Shared services ~ less cost	Security, Isolation, Performance
Expandability	Rapid elasticity (on-demand)	Scalability of legacy systems
Network	Ubiquitous access	Legal Access and Data Storage
Policy	Un-ambiguous specification of system constraints	Fewer barriers to creating ad-hoc environments (cloud mash?)





PwC Survey on Cloud Risks

Please indicate your view on the seriousness of each risk for your organization, on a scale of 1 to 5, where 1 = minimal risk while 5 = extremely serious risk.



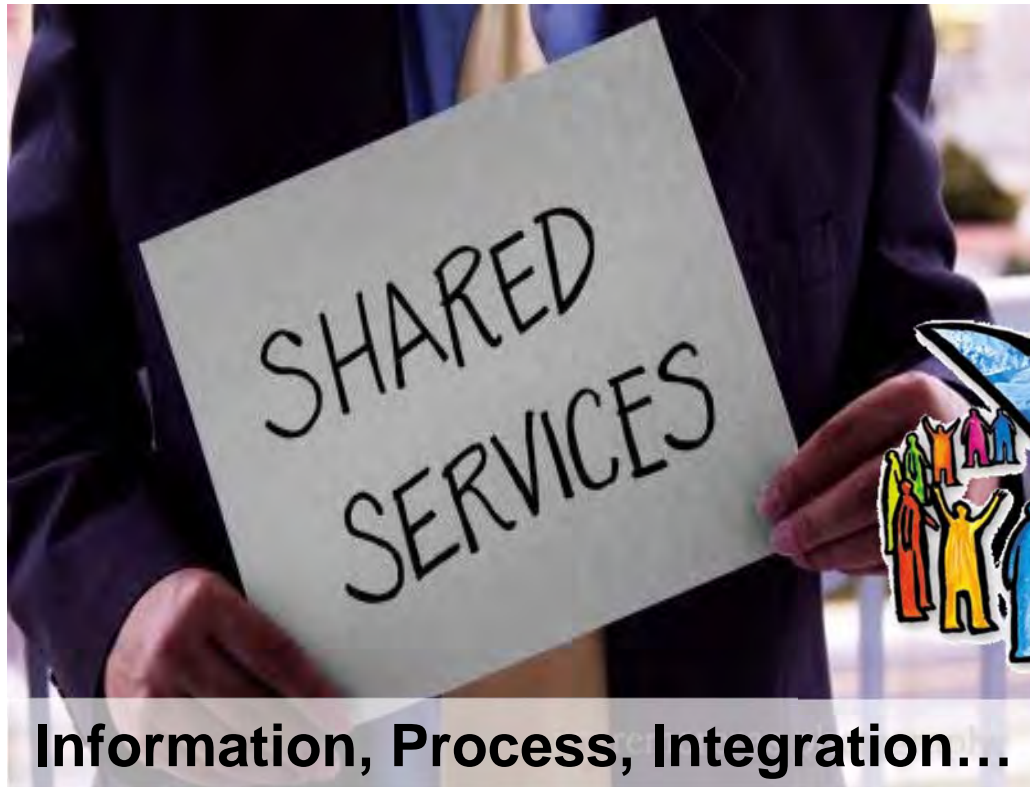
476 respondents – also trust of vendor and no guarantee of service location...





CITY UNIVERSITY
LONDON

SOA Pattern



Information, Process, Integration...

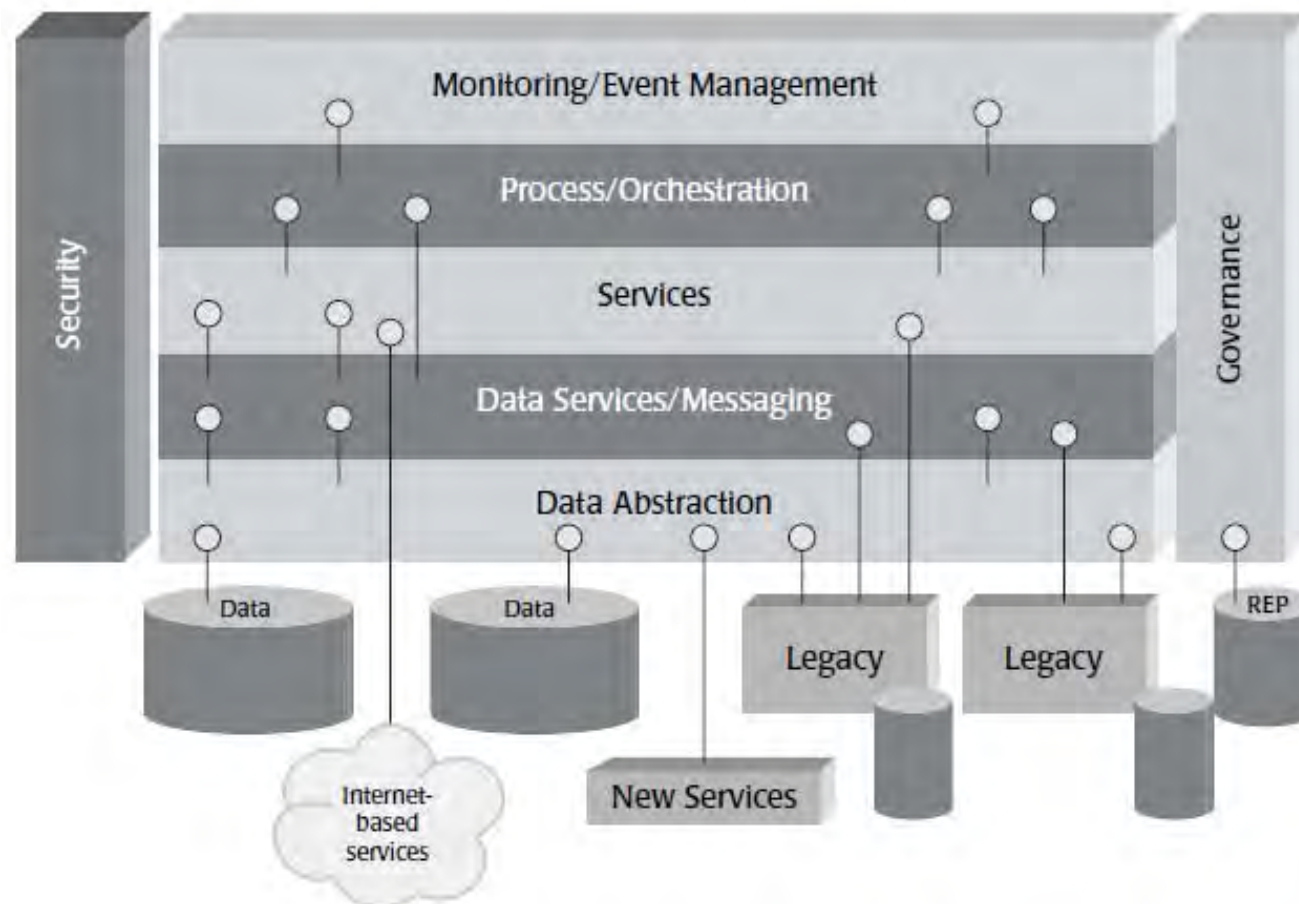


Governance!





SOA Architectural Instance....



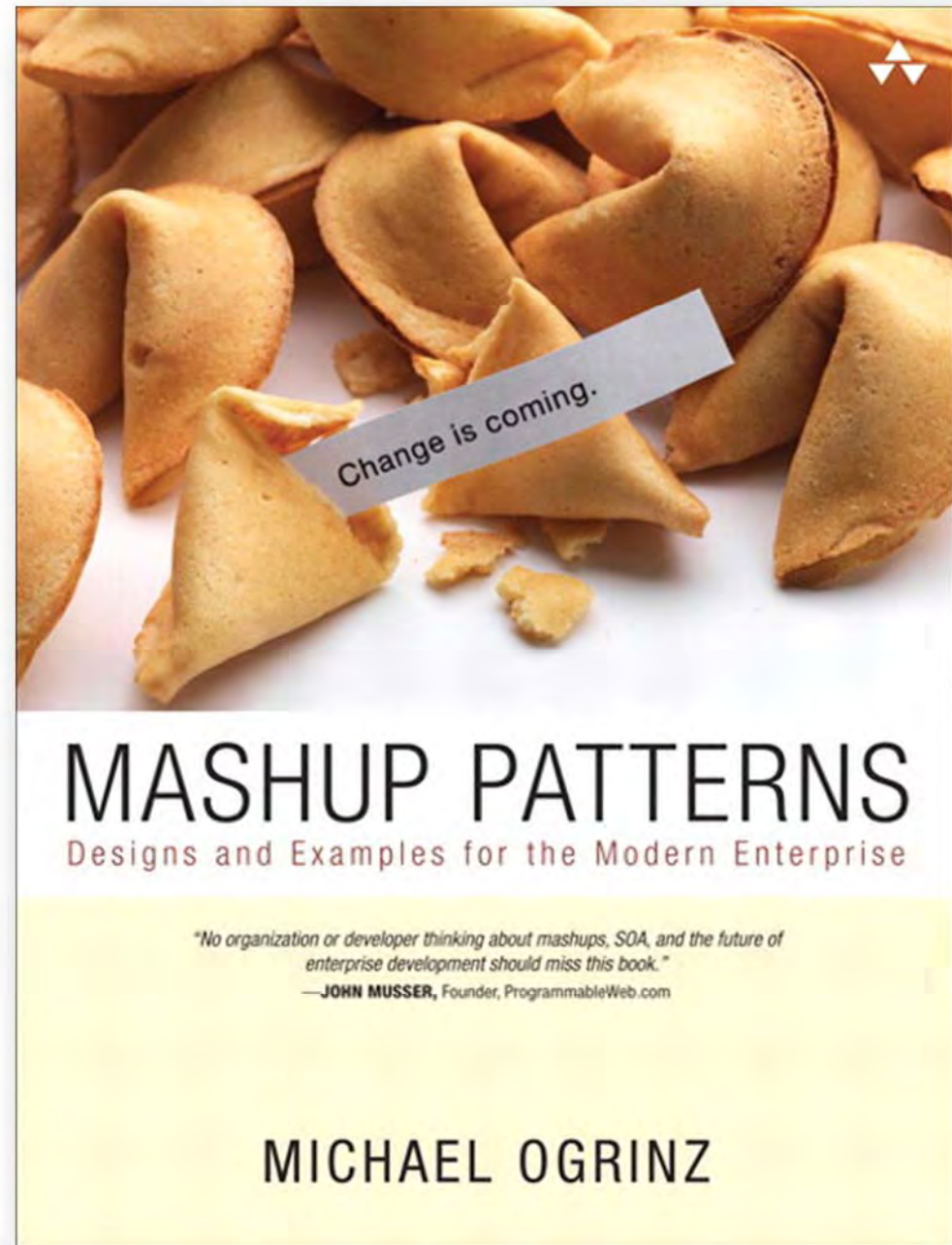
Linthicum 2009



CITY UNIVERSITY
LONDON

“Mash-ups”

“Robust SOA environments are a **hothouse** for mash-up growth, ...that can be mixed together to provide new services.”





CITY UNIVERSITY
LONDON

“Mash-Up” = Ad-hoc Composition?





CITY UNIVERSITY
LONDON

My Cloud-Service-Mashup Dilemma

Agile
vs.
Rigor





CITY UNIVERSITY
LONDON

Propositions

- Support Engineers for
 - Cloud Architectures
 - Service Design
 - Mash-up Safety
- Still do not have concrete disciplines (that can be measured)





CITY UNIVERSITY
LONDON





CITY UNIVERSITY
LONDON

Our focus in engineering support...

Quality of Service Policies	▶ Safety (Process/Deployment)
	▶ Agreements (SLAs/Monitoring)
Compliance Assurance Privacy	▶ Certificates (Privacy/Asserts)



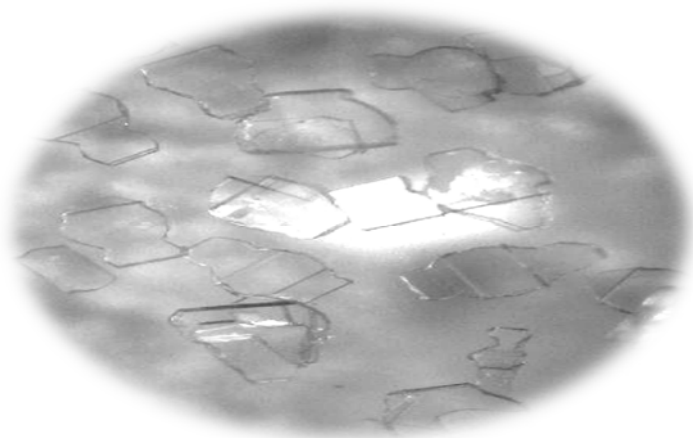
Engineering Support for both Design-time and Run-time aspects





CITY UNIVERSITY
LONDON

Service Safety for Cloud Deployment



*“Predicting polymorphs
in chemical structures”*

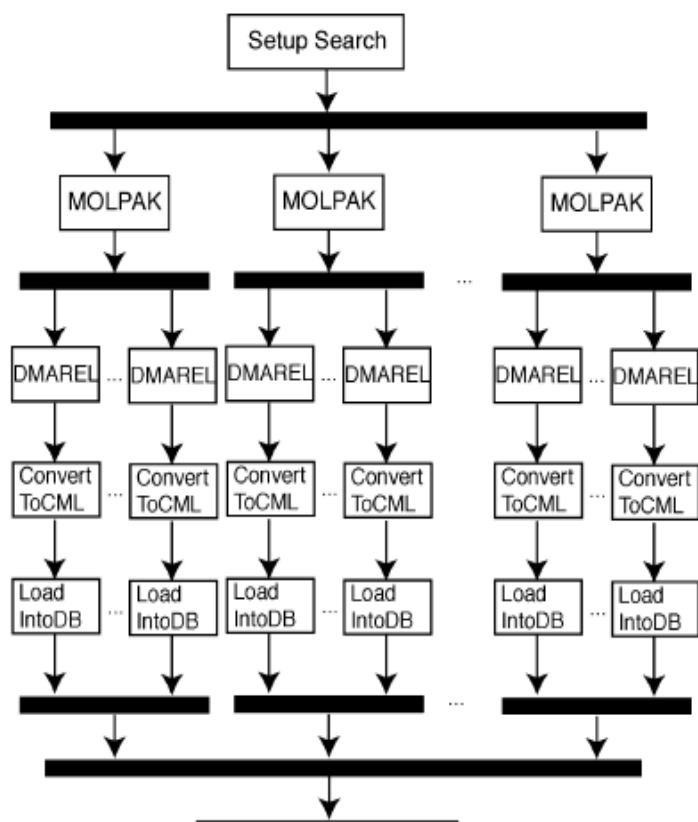
- UCL e-Science
- Private Grid/Cloud
- Chemical Defects
- Service-based
- Expert Analysis

***W. Emmerich et al. Grid Service Orchestration using the Business Process Execution Language (BPEL). Journal of Grid Computing, 2005.**





Overview



- Client MOLPAK
- Invokes ≤ 38 DMAREL
 - Invokes ≤ 200 inspect services
 - Molpak polls for “completed”
 - Repeats for each property
- Up to 7,600 concurrent interactions (5mins-1hr)



CITY UNIVERSITY
LONDON

Safety Checks



- Model-based Analysis
- Service Workflows
 - WS-BPEL Individually
 - Choreography (Interactions)
- Deployed
- **System Error**





Resources

- Check server logs
 - Queuing of service requests
 - Blocked instance creation
- **Thread pool exhausted**
 - Increase resource pool size?
 - Fixed it, but after some time...
- **Threads exhausted again!**





CITY UNIVERSITY
LONDON

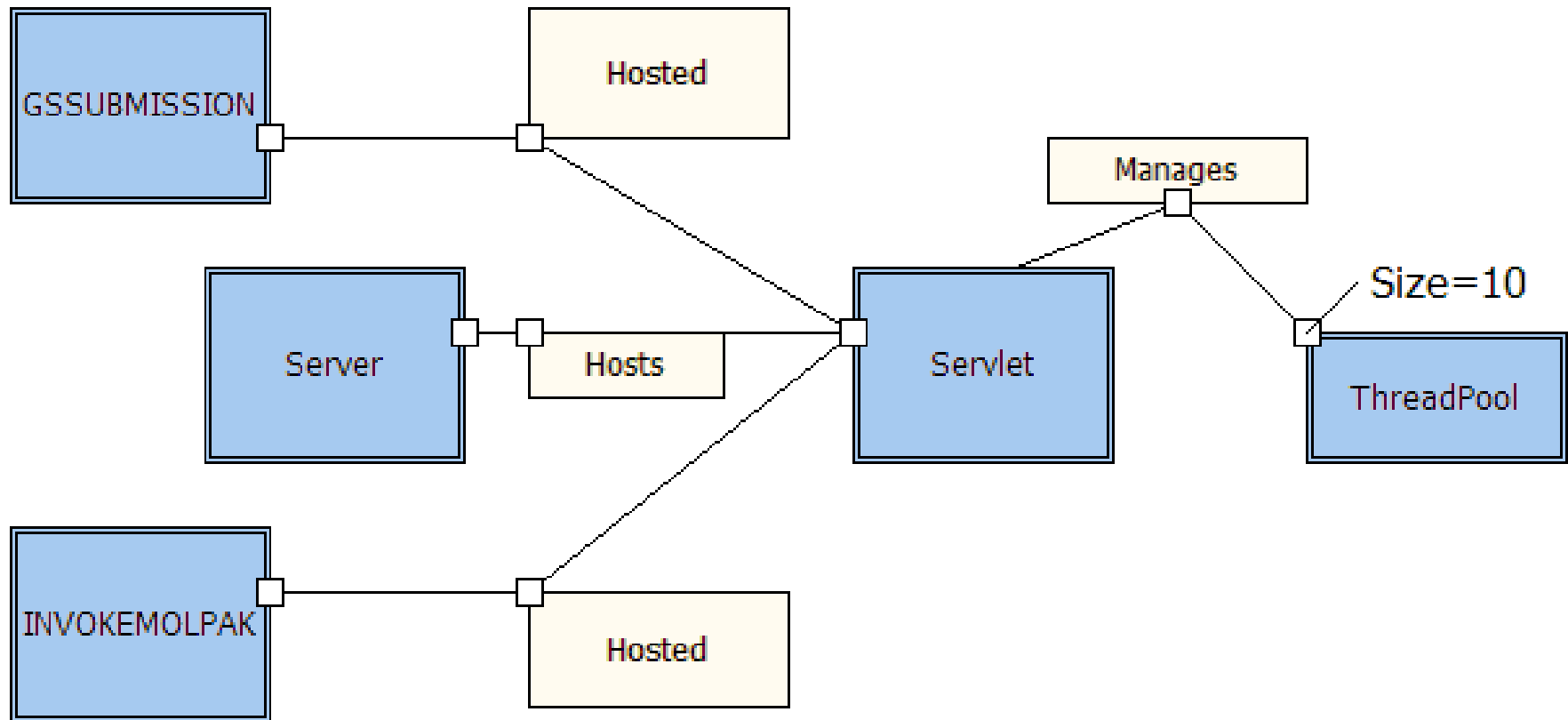
Consideration

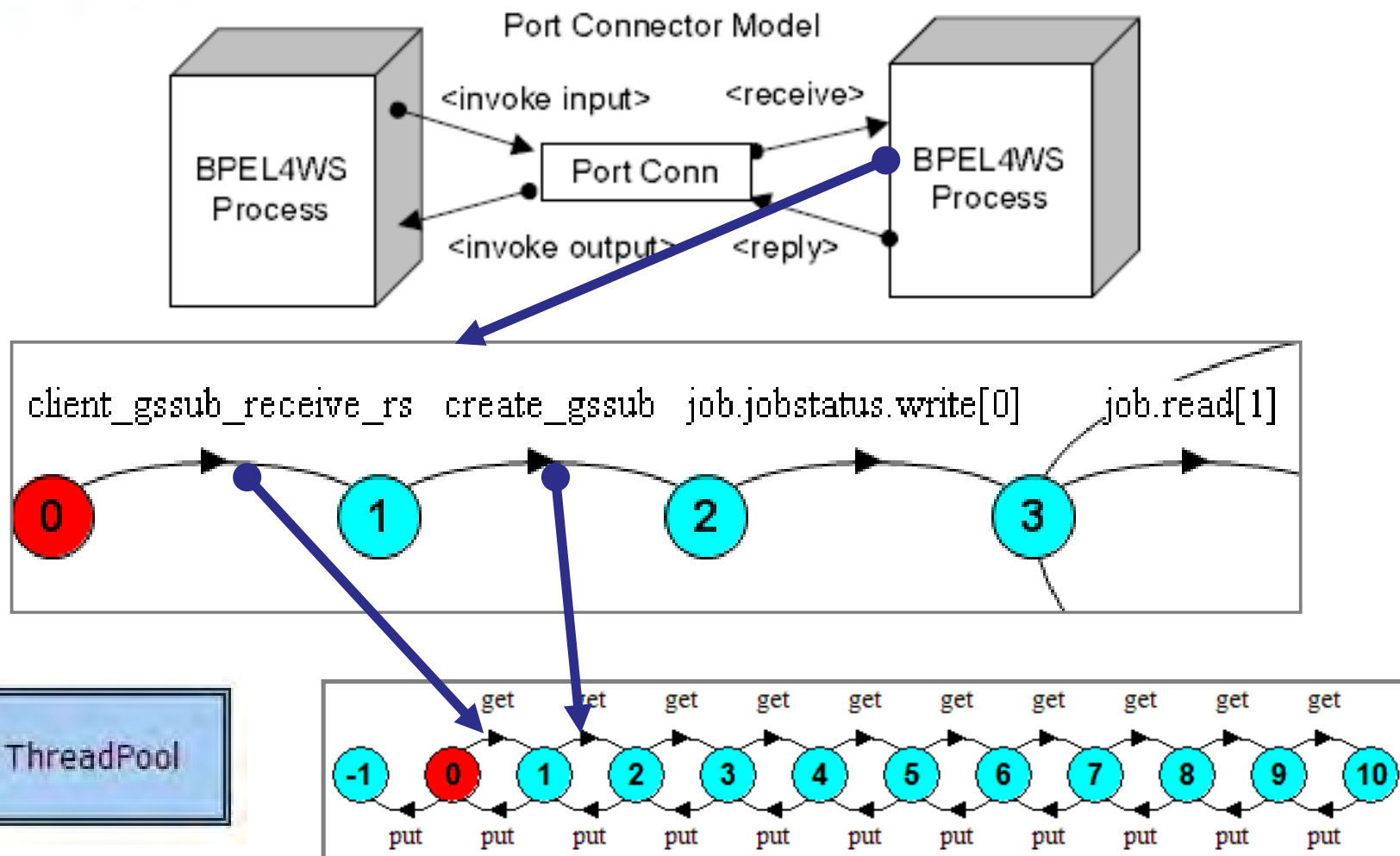
- Architecture + Behaviour
 - Threading mechanism
 - Service synchronization
 - Co-location decision
- Evident at run-time
- Design-time checks?



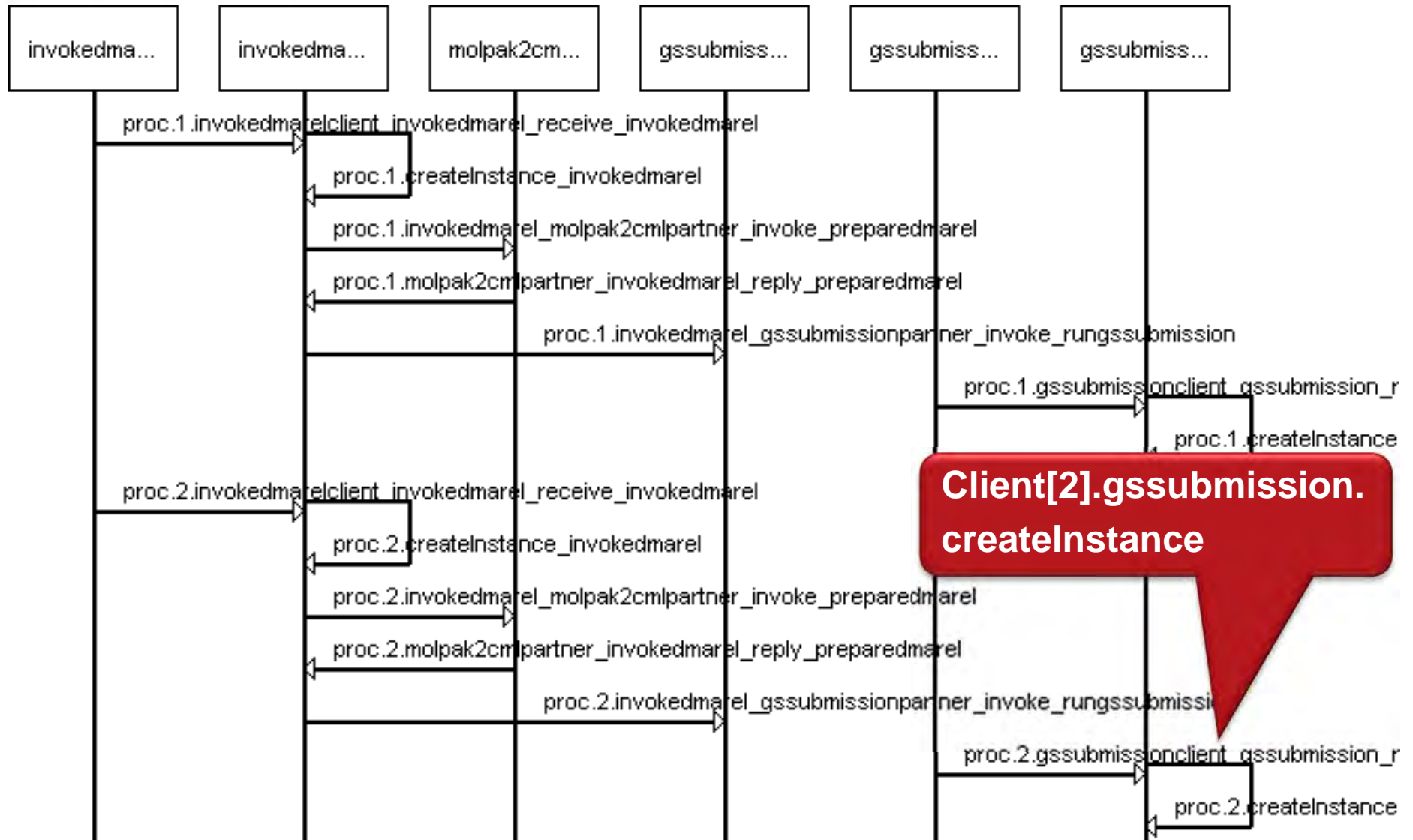


Architecture



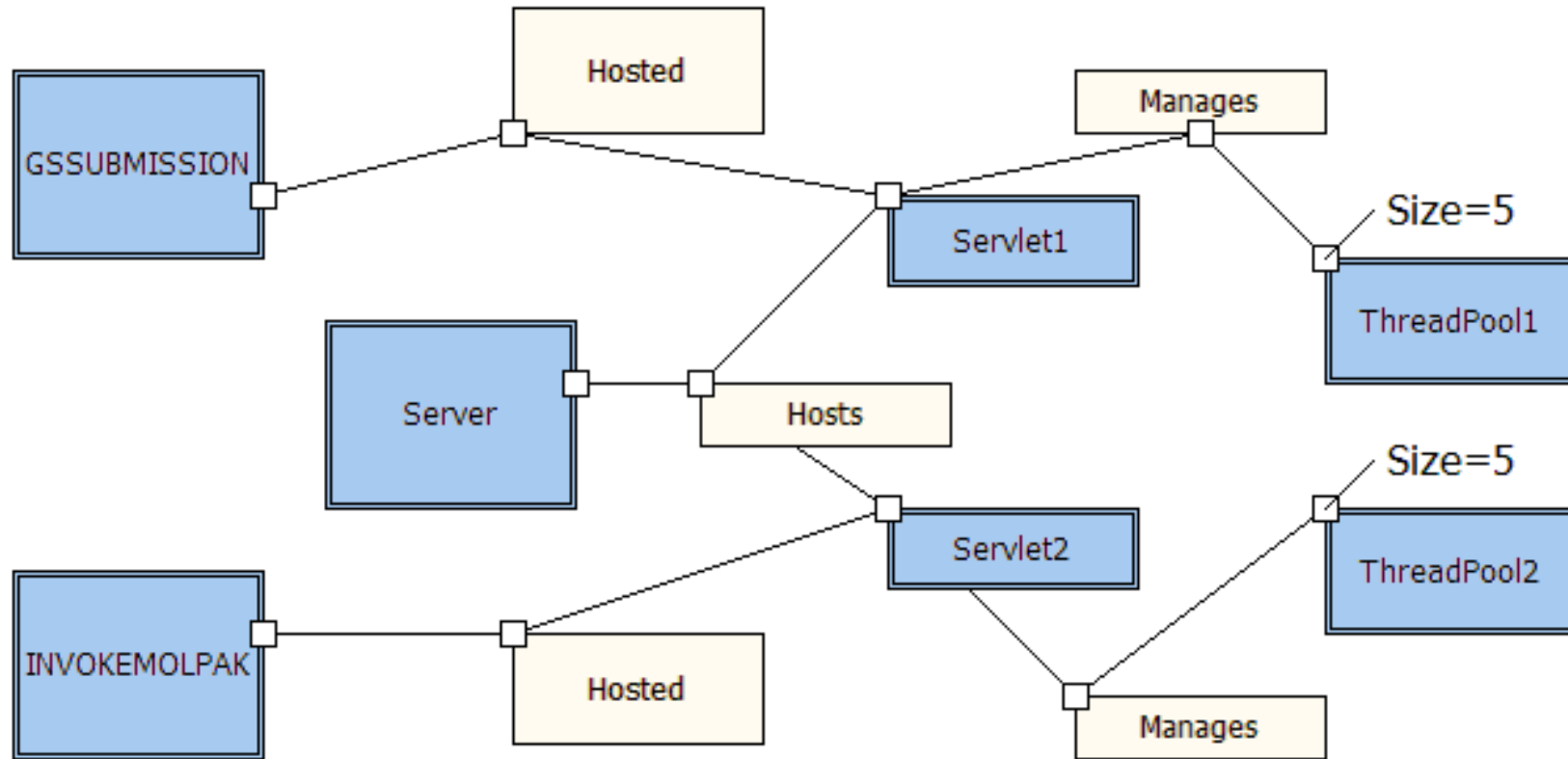


***H.Foster et al. Model Checking Service Compositions under Resource Constraints, in proceedings of ESEC/FSE 2007**





Solutions?





Design Interactions Obligations Deployment Modes

Select Processes and Architecture for Verification

Verify Ready for verification (or add more processes).

1. Architecture Model (UML/xAD2)

Browse UML2 Model Package Loaded.

Model
UML Deployment Model

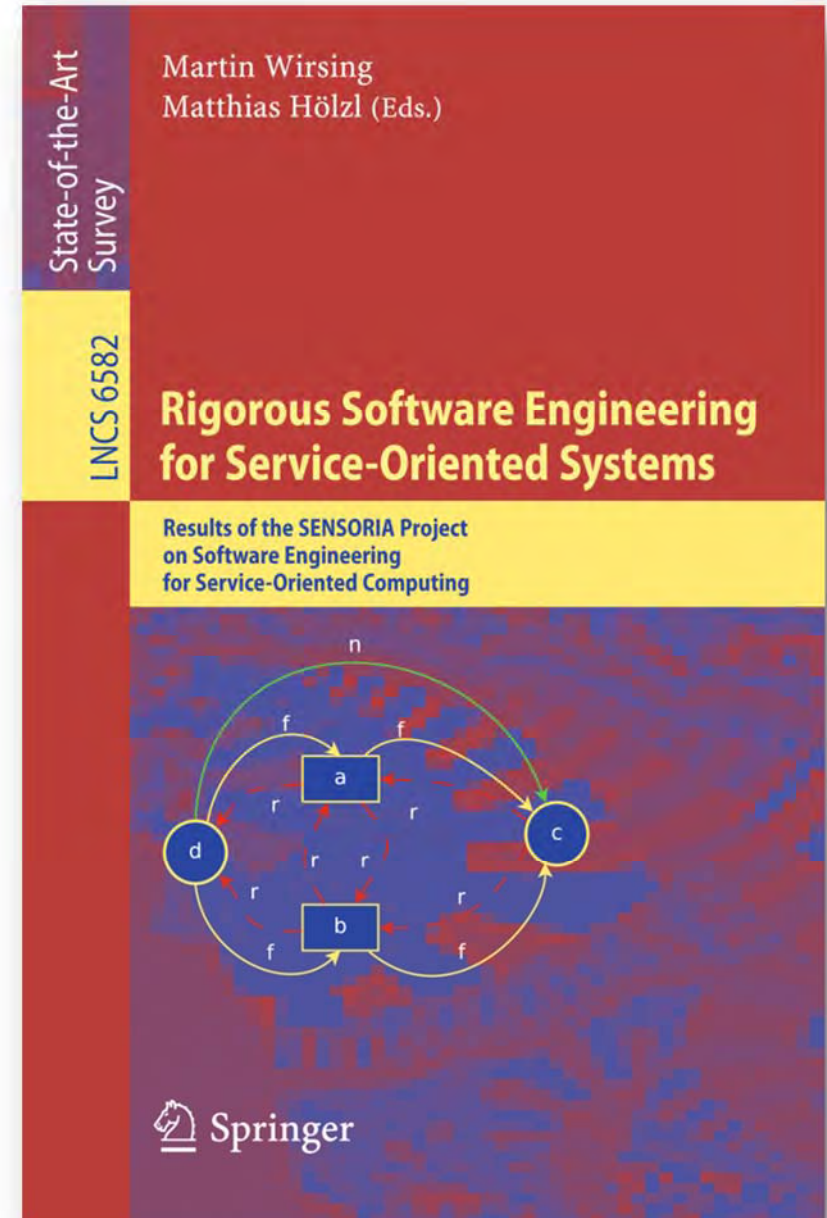
2. Process Source (BPEL/WSDL)

Process	Source	Interface
INVOKEDMAREL	C:\Dev\eclipse...	C:\Dev\eclipse...
GSSUBMISSION	C:\Dev\eclipse...	C:\Dev\eclipse...



CITY UNIVERSITY
LONDON

Further details...

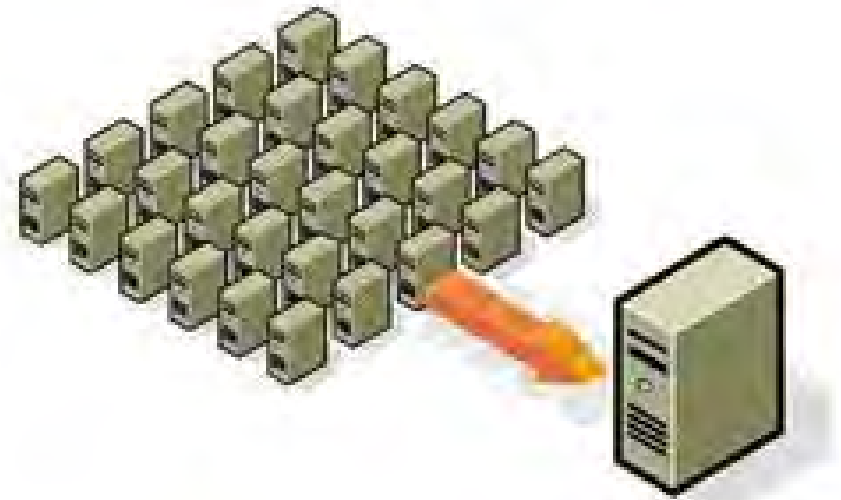




Virtualisation Alert!

- Solves some issues
 - Local (resource) protection
 - Virtual servers still resources
 - Also have shared services
 - Composition of servers

- Security and Safety Issues remain...





CITY UNIVERSITY
LONDON

SLAs for Cloud Computing

- Negotiation
- Agreed Policies
- Constraints
- Monitoring
- Adaptation





CITY UNIVERSITY
LONDON

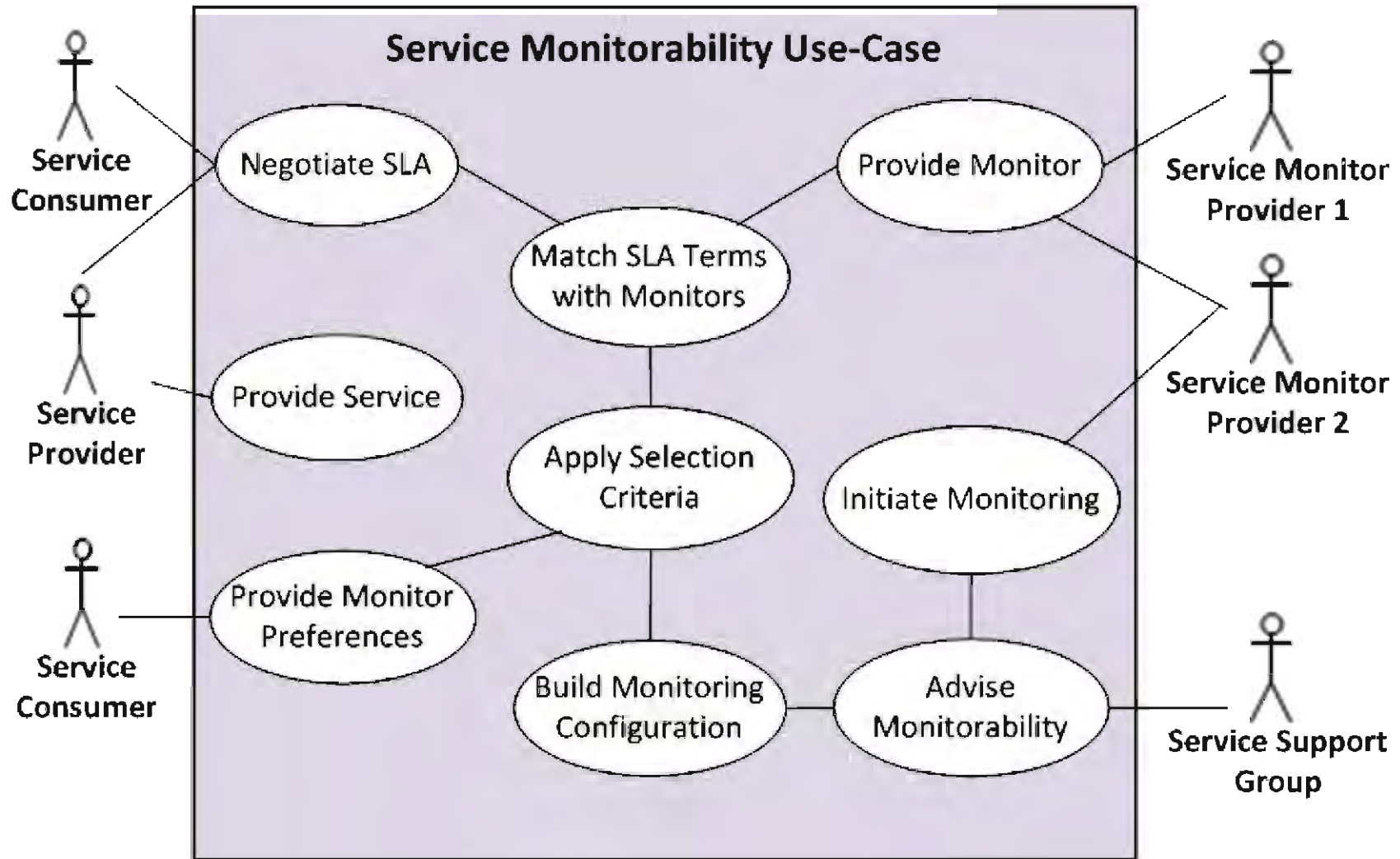
SLA@SOI

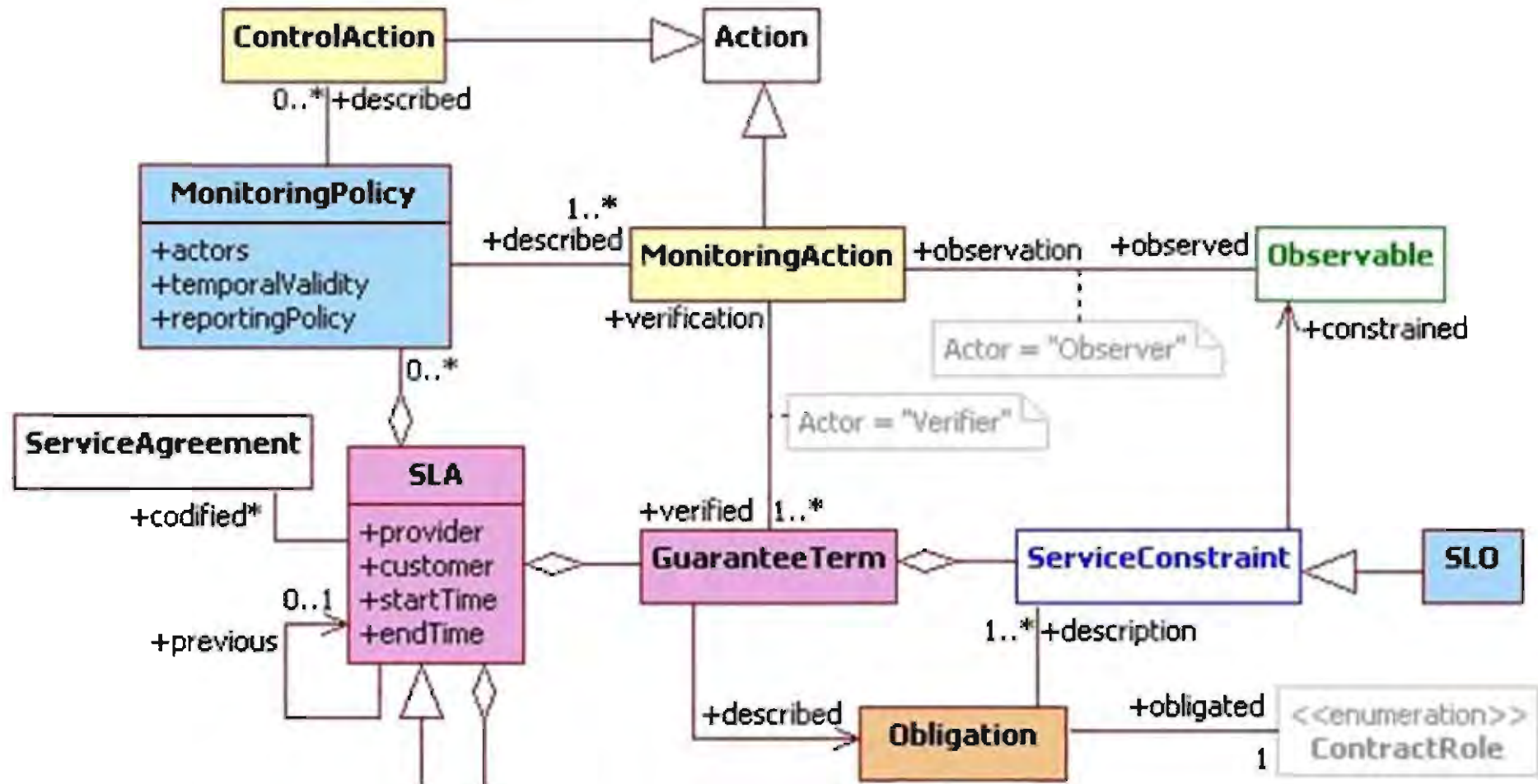


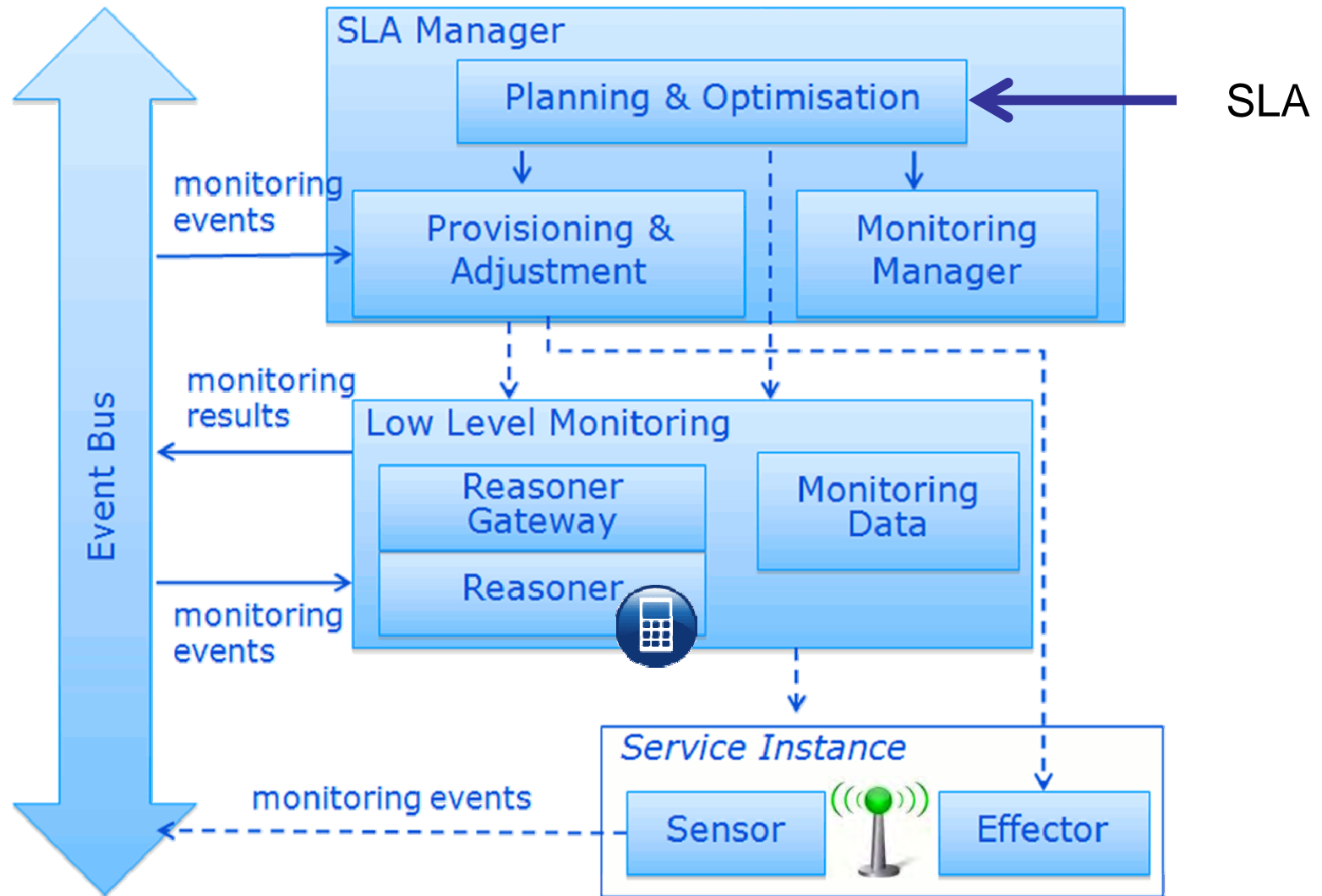
*SLAs Empowering a
Dependable Service Economy*



- EU ICT FP7 Project (Oct07-Oct11)
- 12 Partners, 15mil EUR
- Embed SLA Framework in SOA/Cloud Inf.

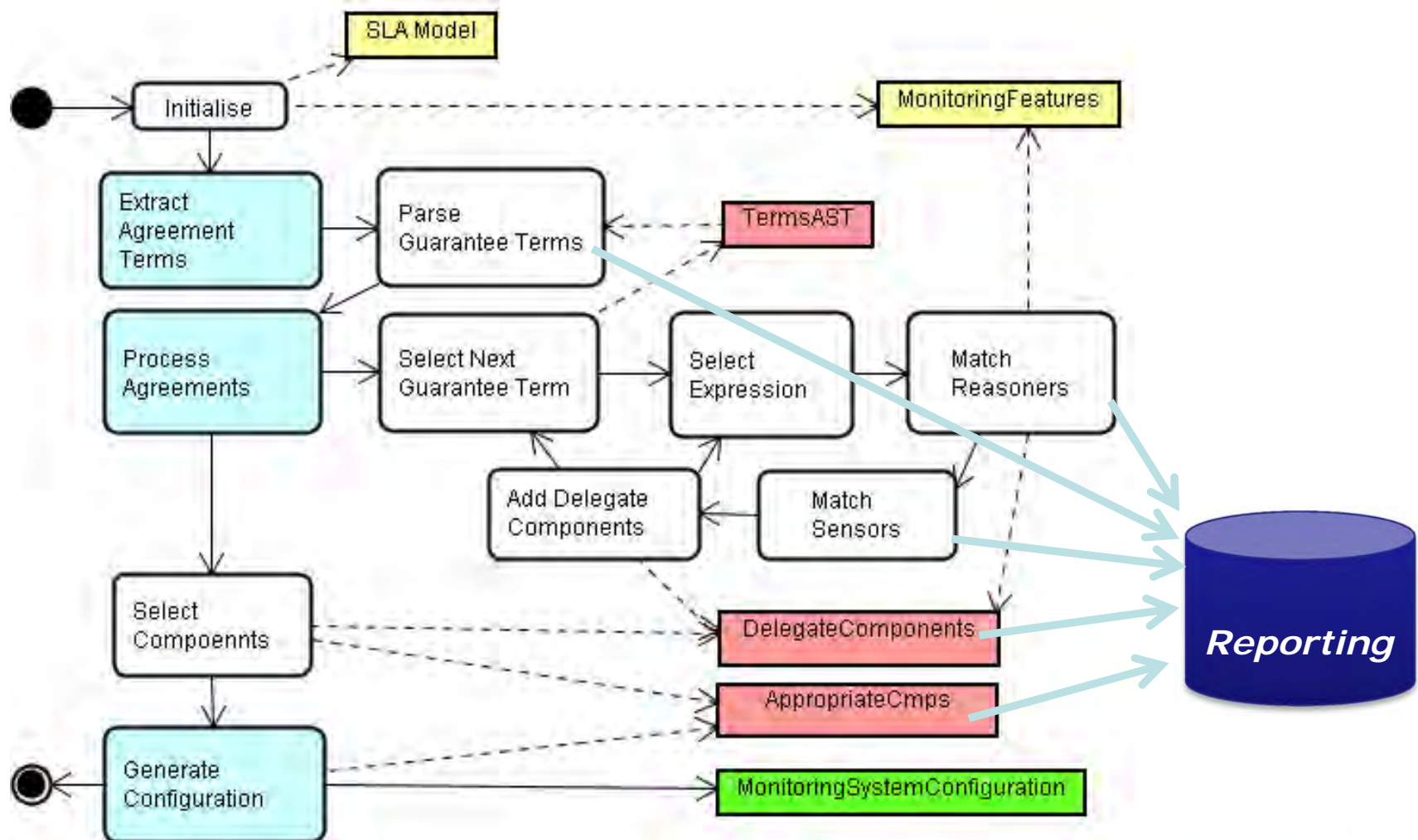








Monitoring Manager





Monitorability Manager

SLA @ SOI Monitorability Reporting

Overview | Terms | Configuration

SLA

Select SLA

Selected SLA: B4_SLA.xml

Monitoring Features

Select Feature Set:

B4-Features

Add Features

Monitorability

Check Monitorability

Agreement Summary

Agreement Term	Status
autogen	Not Monitorable (see Indicators)
ServiceWideGuarantees	Monitorable

autogen Status Indicators

Result	Description	ID	Step	Type	Path	Value
ERROR	No CMF matched for...	http://www...	MATCHING...	MATCHING	autogen/V...	http...

autogen CMF Provider Summary

Component ID	Type	Features
777e8400-sss2-41d4-a716-406075043333	REASONER	
555e8400-sss2-41d4-a716-406075043333	SENSOR	

Log

Step	Type	Report	Result	Class	Line	Warnings
ASTTerms	DEBUG	Guaranteed Sta...	Passed	org.slasoi.gsla...	152	
ASTTerms	WARN	Guaranteed Sta...	Issue	org.slasoi.gsla...	152	
ASTTerms	ERROR	Guaranteed Sta...	Failed	org.slasoi.gsla...	152	



The screenshot displays the SMART Workbench interface, which is used for SLA (Service Level Agreement) management and monitoring. It is divided into several panes:

- Project Explorer:** Shows the project structure for 'ORC-Business', including files like 'ORC_Business-SLA.xml' and 'ORCLandscape.scm'.
- ORCLandscape.scm:** A tree view showing the landscape structure, including 'Landscape', 'Service Type - ORC_ServiceType - (providedTypes)', 'Service Implementation - ORC_AllInOne', and 'Virtual Appliance ORC_DB'.
- SMART: Monitorability Reporting:** A tool for generating reports. It includes sections for:
 - 1. SLA:** 'Select SLA' (set to 'ORC_Business-SLA.xml') and 'Agreement Summary' table.
 - 2. Monitoring Features:** 'Select Feature Set' (set to 'ORCBFeatures') and 'ORC_ResponseTimePayment Status Indicators' table.
 - 3. Monitorability:** 'Check Monitorability' button and 'ORC_ResponseTimePayment CMF Provider Summary' table.
- EVEREST Monitoring (RCG):** A tool for monitoring RCG (Resource Configuration Graph). It includes:
 - Control:** 'Guarantee Terms' and 'EVEREST Rules/Assumptions' sections.
 - Monitoring Results Summary:** A table with columns for 'Guarantee Term ID', 'Decision', and 'Time'.
 - Related Events:** Fields for 'Guarantee Term ID', 'Guarantee Term Status', and 'Variable Bindings'.
 - Log:** A table with columns for 'Time', 'Data', and 'Info'.



CITY UNIVERSITY
LONDON

Further details in...



projects/sla-at-soi

Philipp Wieder · Joe M. Butler
Wolfgang Theilmann
Ramin Yahyapour *Editors*

Service Level Agreements for Cloud Computing

Foreword by
Jessica McCarthy

 Springer



CITY UNIVERSITY
LONDON

Compliance, Assurance, Privacy

- Certification of Services
- Models, Languages...
- Applications
 - Security and Privacy
 - Functional Assurance
 - Mechanically certified





CITY UNIVERSITY
LONDON

Certification

ASSERT4SOA

Advanced Security Service cERTificate for SOA

- EU ICT FP7 Project (Oct10-Oct13)
- 6 Partners, 5.4mil EUR
- Why is certification useful?





CITY UNIVERSITY
LONDON

Certificates

- Increased User Trust
 - e.g Attests Security, Build, Safety
- Evaluating Services
 - Modeling and Testing by Experts
 - Assumes Trust in Expert
- **Currently a manual process**
 - Changes require re-certification





BSI-DSZ-CC-0536-2010

Operating System

Apple Mac OS X 10.6

from

Apple Inc.

PP Conformance:

"Controlled Access Protection Profile" (CAPP)
Version 1.d, 8 October 1999

Functionality:

Common Criteria Part 2 extended

Assurance:

Common Criteria Part 3 conformant
EAL 3 augmented by ALC_FLR.3



Common Criteria
Recognition
Arrangement



The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any





CITY UNIVERSITY
LONDON

ASSERTs

- A digital certificate of properties (e.g. x.509, SAML...)
- ASSERT4SOA:
 - ASSERT-E: Test Evidence-based
 - ASSERT-M: Formal Model-based
 - ASSERT-O: Ontology-based
- Designed for mechanical processing
 - Machine-readable, semantics of certification



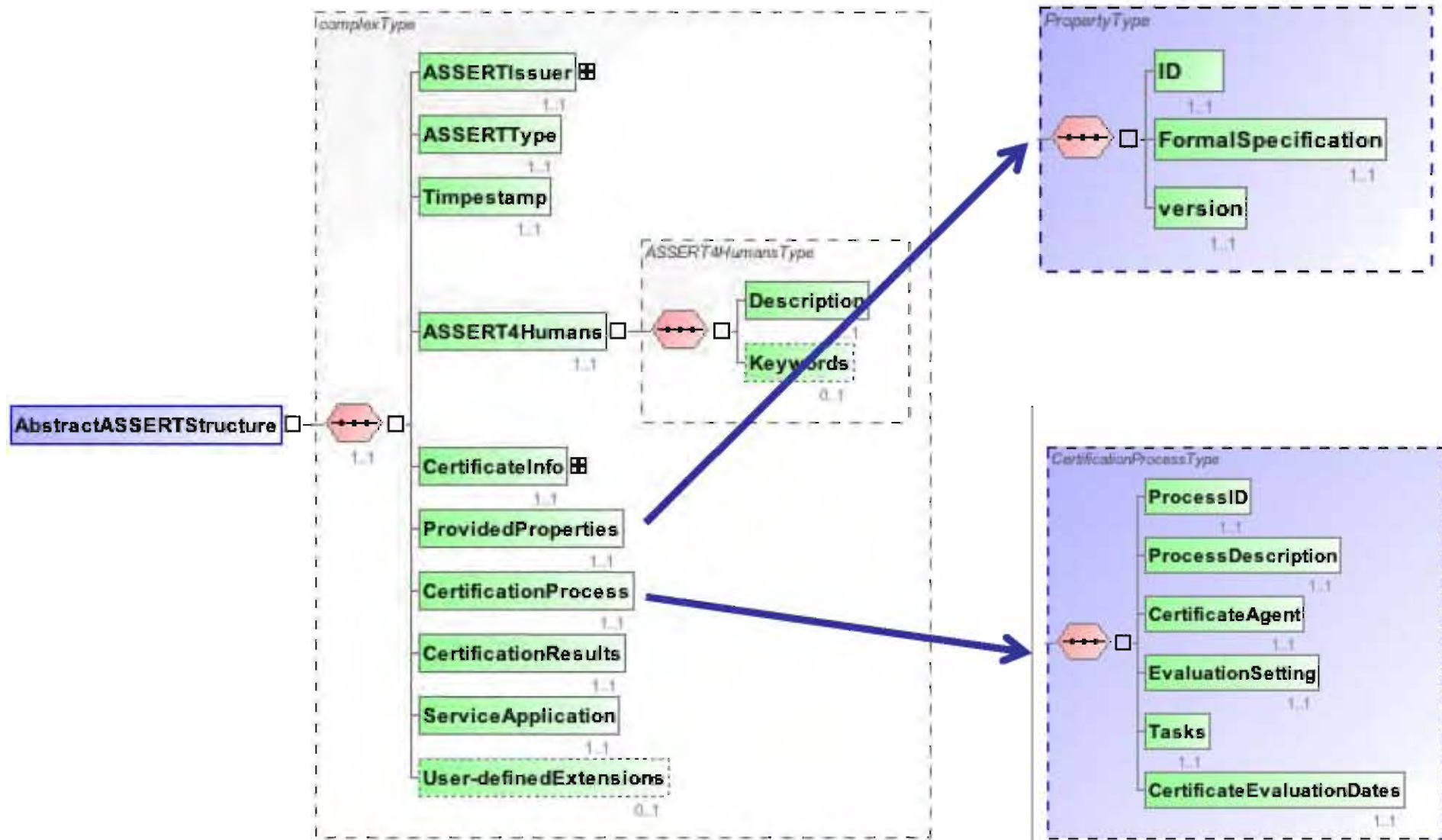


CITY UNIVERSITY
LONDON

ASSERT Language

- Common Core
 - Certification Process
 - Certification Results
- Target Service/Application
- Process of Certification
 - E.g. Security, Safety, Trusted Environment

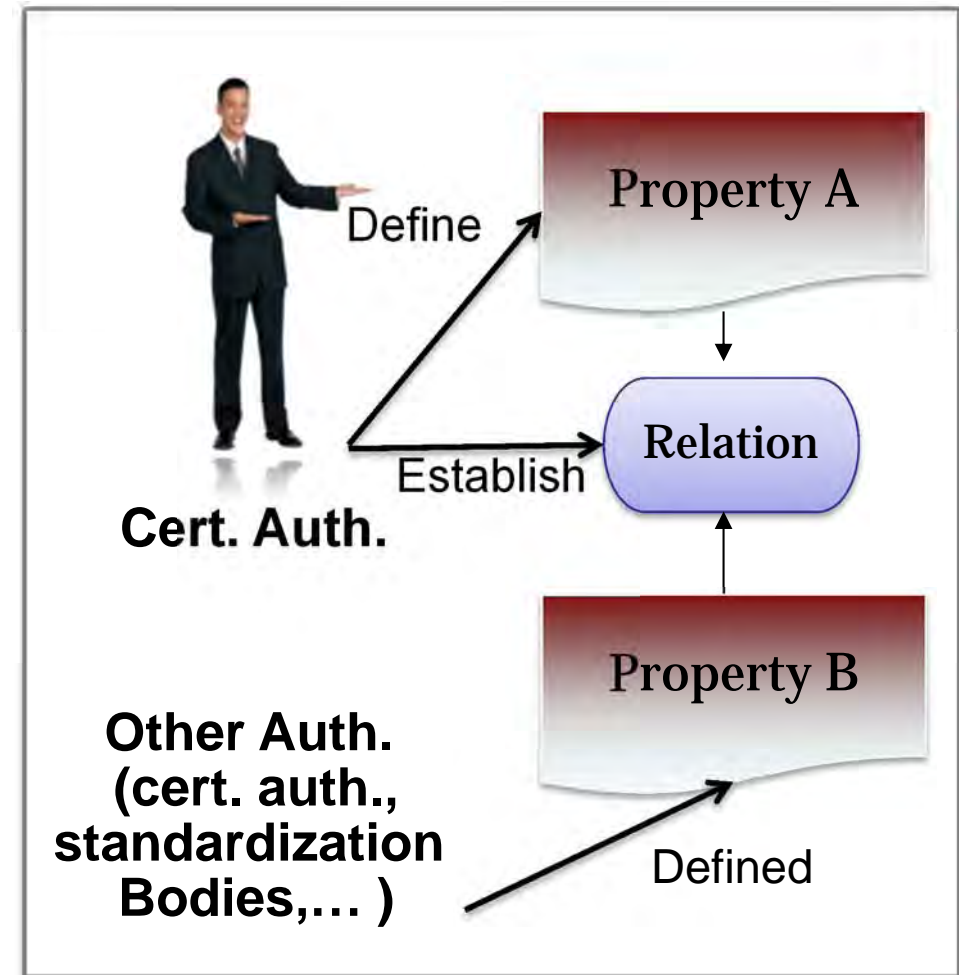






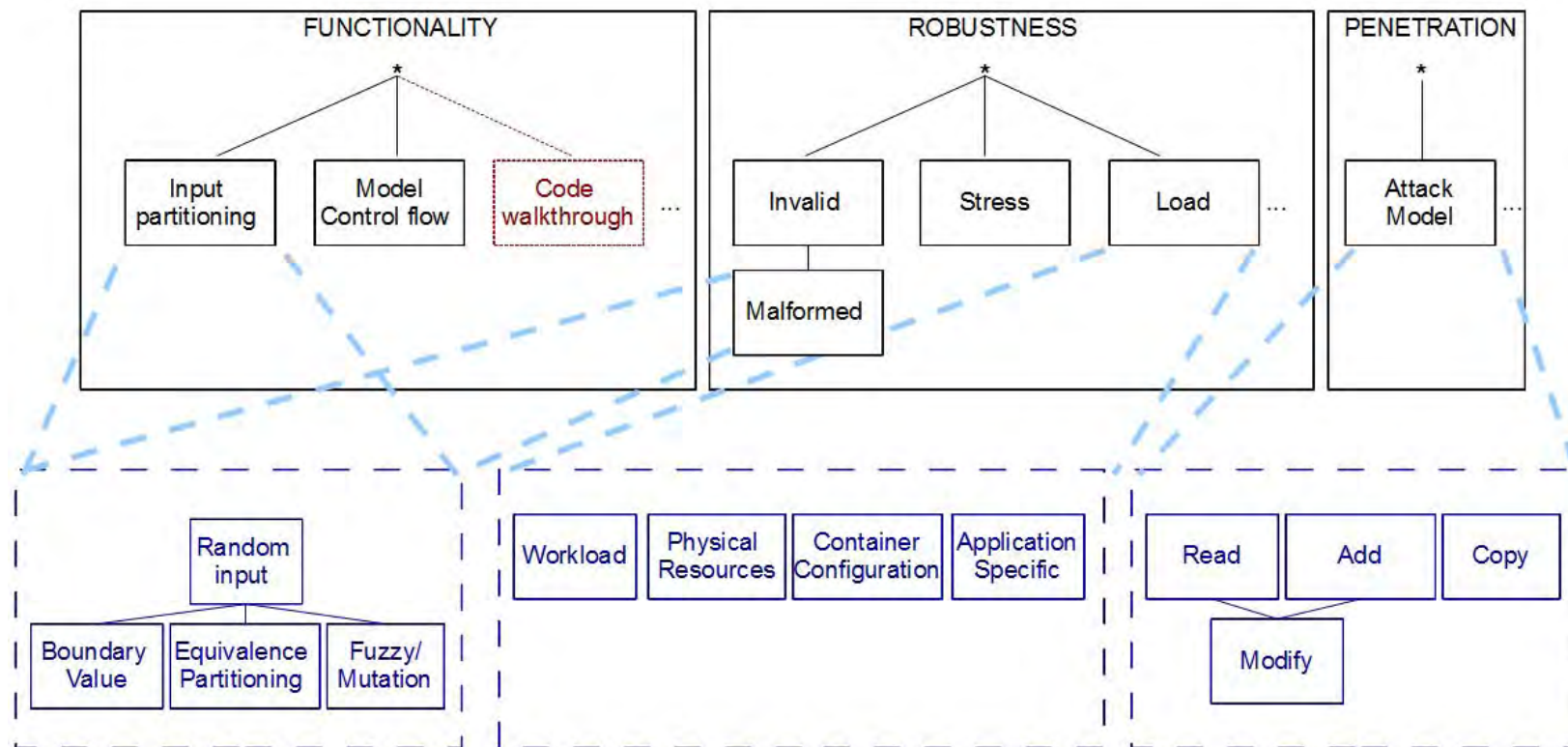
ASSERT Semantics

- Different languages
 - Properties
 - Legislation
 - Cultural
 - Technical
- ASSERT Ontology





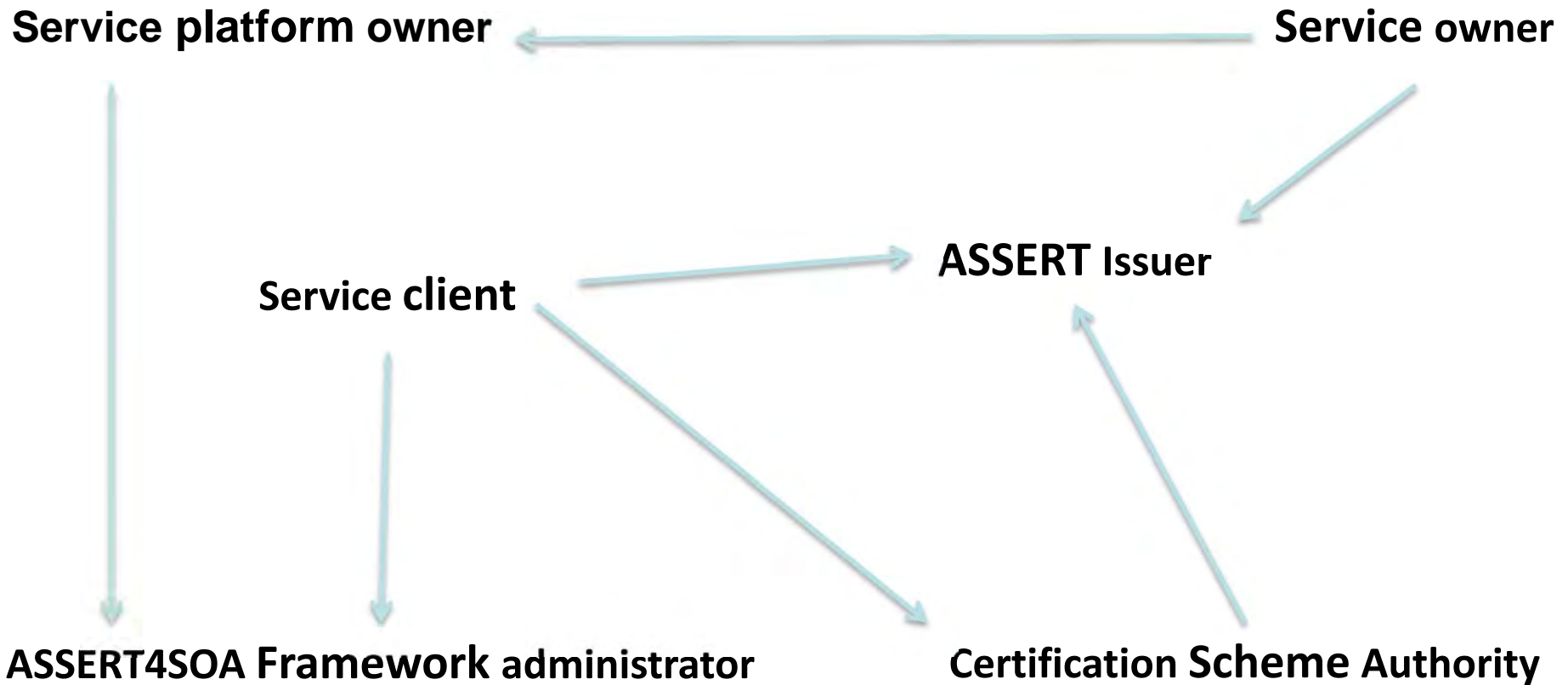
Testing Quality “as-a-Service”?



from *Design and description of evidence-based certificate artefacts for services*,
Deliverable 4.1, ASSERT4SOA Project, October 2011



ASSERT4SOA Vision





• Service

• WSDL

• Abstract service
interface

• Service binding

• endpoint



Certificate: applies to all instance of service (regardless of the endpoint that can be accessed)

[Service Type Certificate]

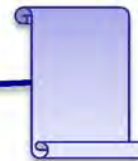
Certificate: applies to

- the specific instance of service that is accessible from the particular endpoint

[Service Instance Certificate] OR

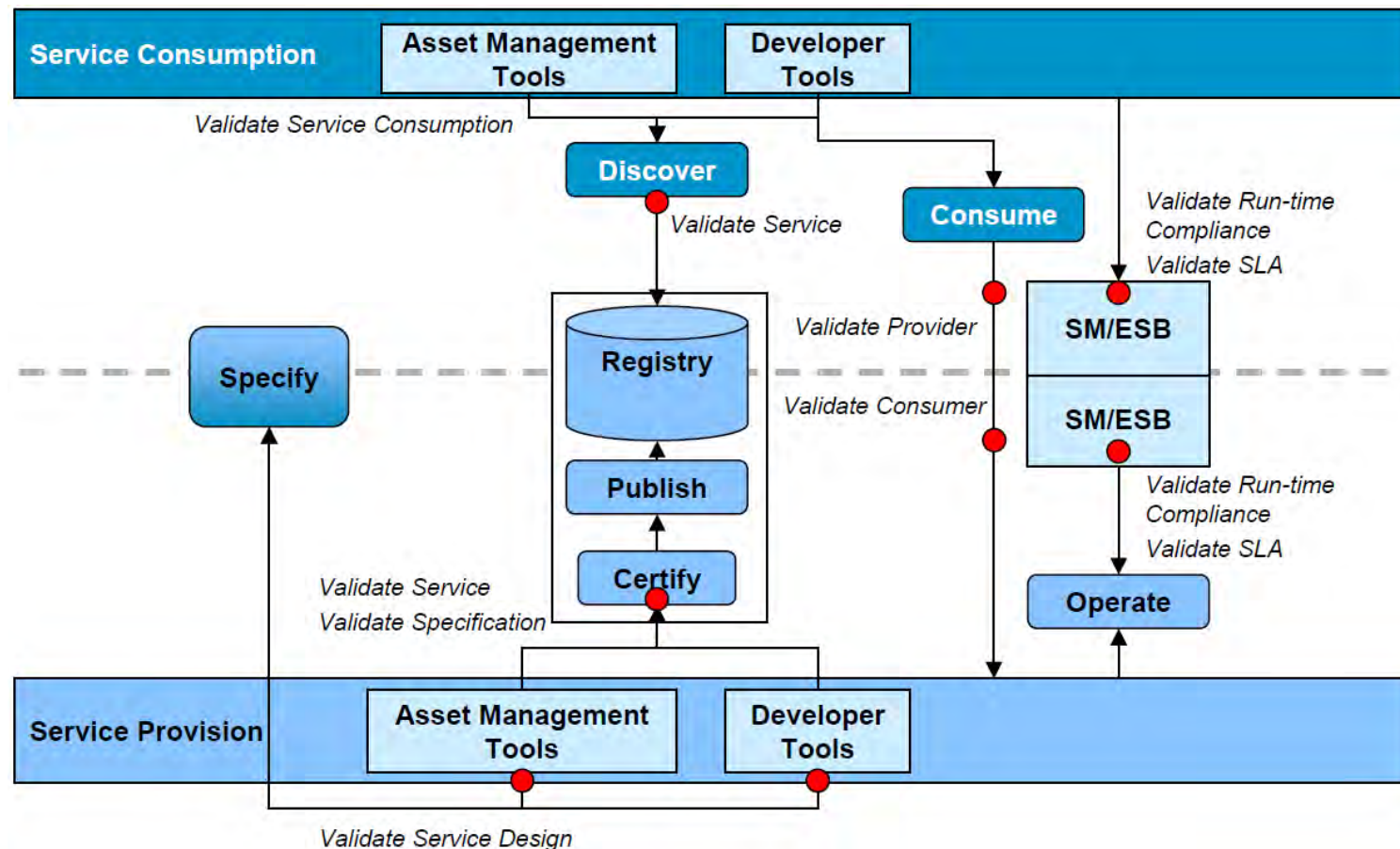
- The container where the service instance is deployed

[Service Container Certificate]





Certification and Validation





CITY UNIVERSITY
LONDON

Application of ASSERT4SOA

- Semantics
- Properties
- “Testing-as-a-Service”
 - ASSERT-E: Evidence-based
 - Build, Safety etc...
 - Automated (re)Certification
- “Governance-as-a-Service”





CITY UNIVERSITY
LONDON

Summary

- Service Engineering
 - Issues in compliance (esp. **mash-ups**)
 - Safety Properties
 - Monitoring Services
 - Certificates and Assertions can help
- **Effective only with Governance and Metrics**





CITY UNIVERSITY
LONDON

My Vision? Certified “Baked” Mash-ups!

Some indication of **risks** if mashed...

Certified for Security, Safety and Function

Monitored by default

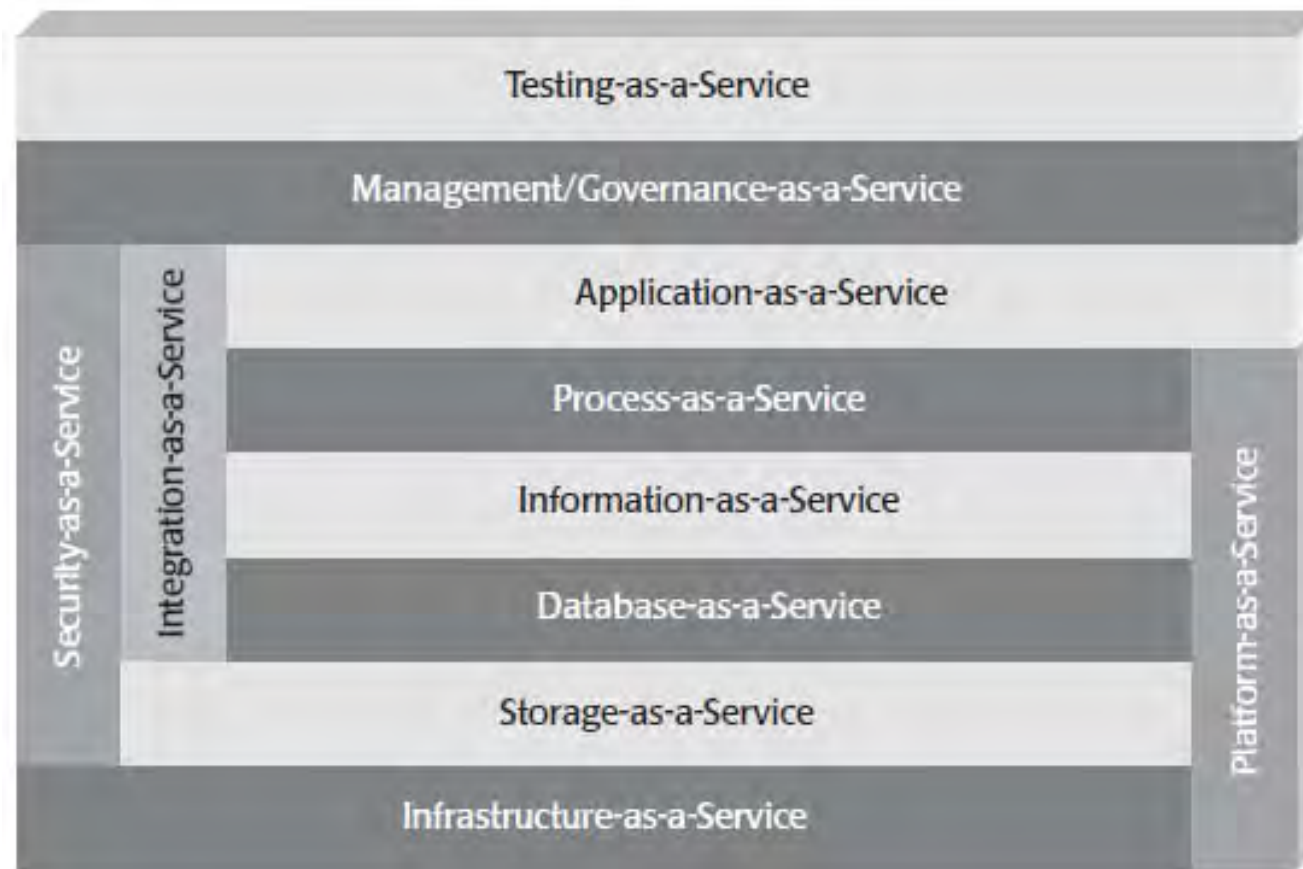
Trusted?





CITY UNIVERSITY
LONDON

Near Future Cloud Support?





CITY UNIVERSITY
LONDON

Questions?

