SOA Governance

Dr Mark Little

Technical Development Manager, Red Hat

Architectural requirements

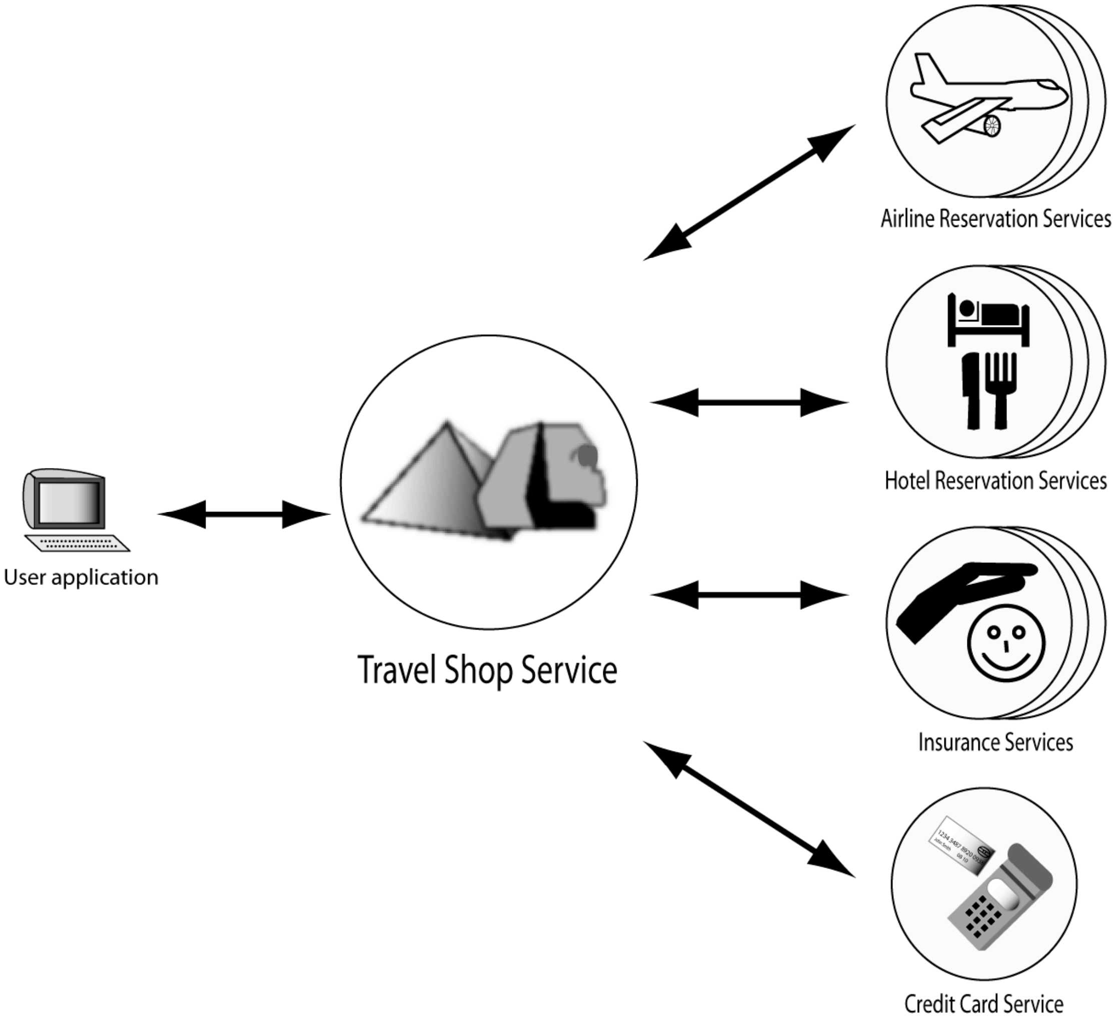
Governance

- **Monitoring and managing distributed systems is complex**
  - No concept of “now”
  - Failures, network partitions etc.
- **SOA makes things more difficult**
  - No control over infrastructure
  - No notion of trust
  - Indeterminate delays
- **Governance is critically important**
  - What services are running?
  - What are their contracts?
  - What are SLAs?
    - Are they being violated?

Service Lifecycle

- **Services go through four phases:**
  - Model
  - Assemble
  - Deploy
  - Manage
- **Lifecycle management concentrates on the development and deployment of services**
  - Is affected by its relationship with other services
- **Governance brings access control, policies etc. into the way in which services are used within a business process**

Composite service



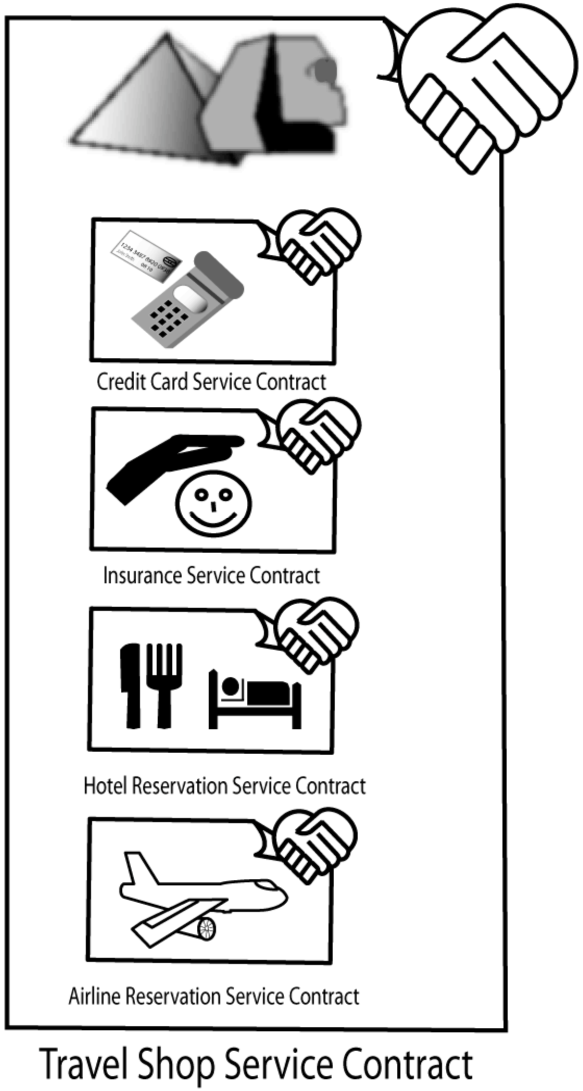
Governance role

- **Affects all of the lifecycle phases**
  - Not just runtime management
- **Good governance solutions should be extensible**
  - What needs to be monitored may need to change
- **Should leverage existing SOI**
  - No separate approach to fault tolerance, reliability etc.
    - Who monitors the monitors?
- **Standards compliance**
  - Replace components with other compatible implementations

Contracts, policies and SLAs

- “Is this service really offering what I want?”)
- “Is this service really doing what it said it would?”
- Composition of services has an affect
- What is a contract?
  - **The service interface**
  - **The messages it can accept, their formats**
  - **A legal contract entered into when using the service**
- The difference between a policy and a contract is that the latter is an agreed policy between service and user

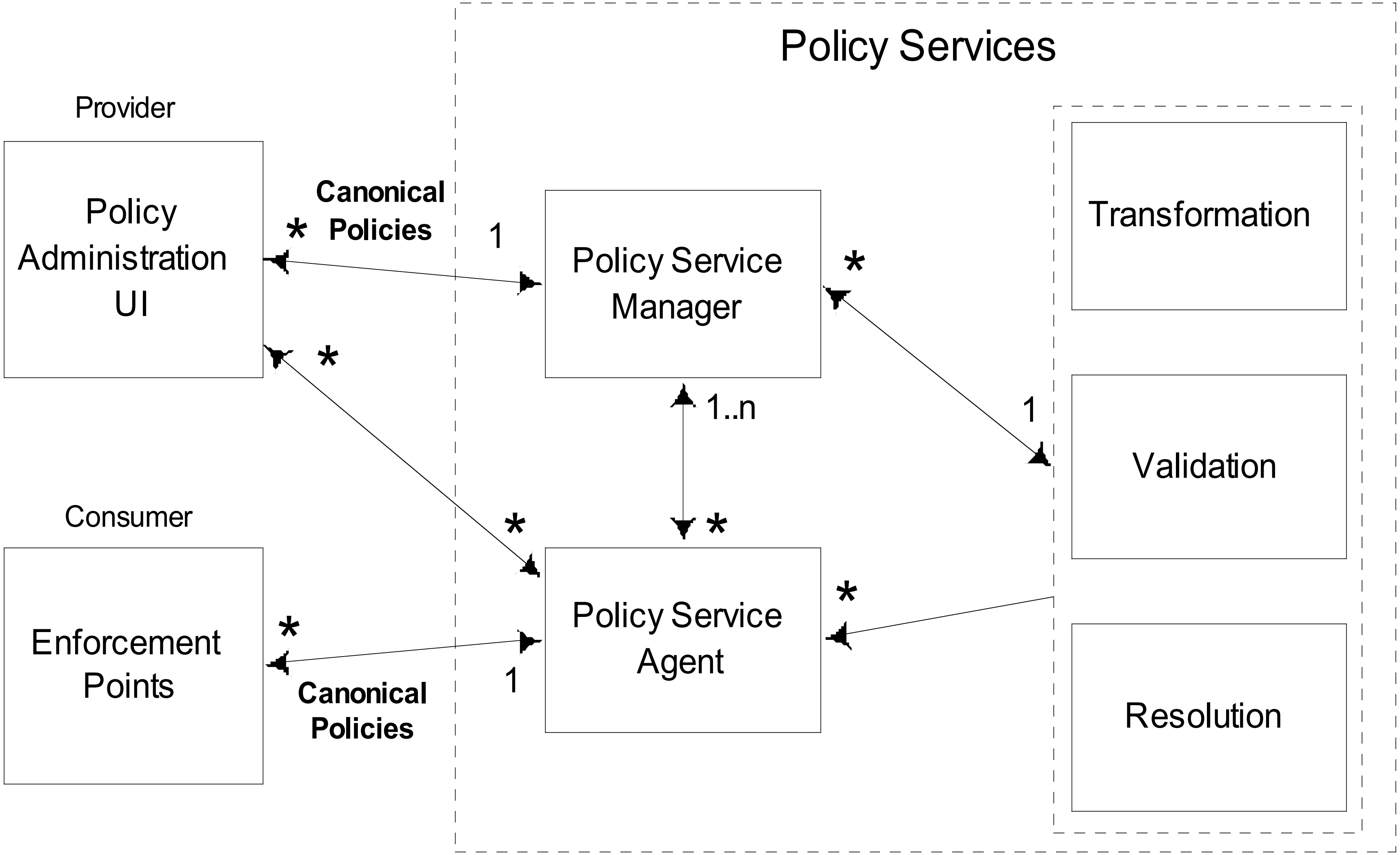
Composite SLA


Credit Card Service Contract
Insurance Service Contract
Hotel Reservation Service Contract
Airline Reservation Service Contract
Travel Shop Service Contract

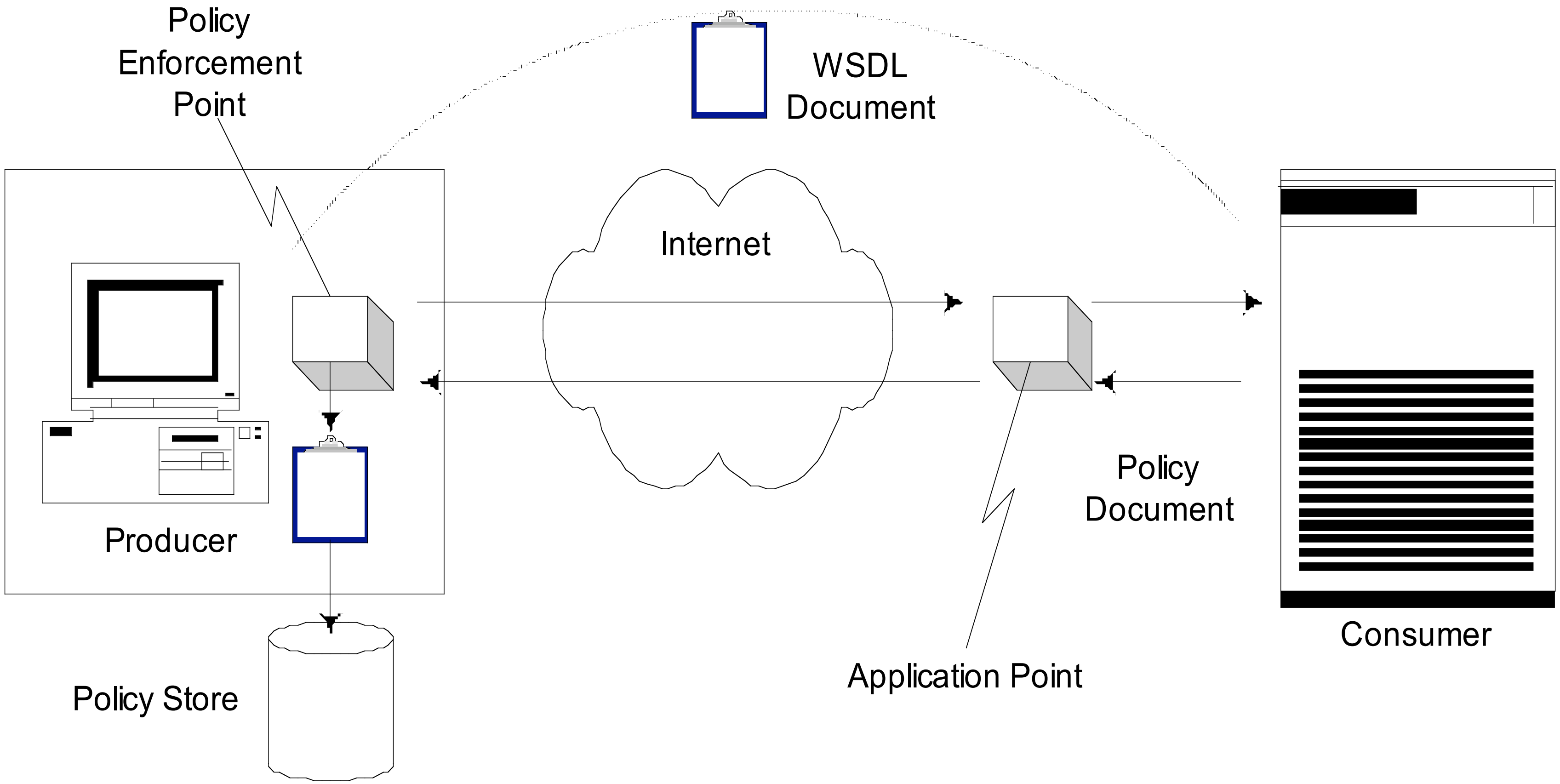
Policies

- **No policy support**
  - The need for policies must be defined outside of the ESB and communicated using ad hoc techniques
- **Definition of policies**
  - Capture and creation of policies at design-time (typically via a graphical interface) and run-time (usually through an intermediary such as a registry)
- **Management of policies**
  - The policies of services to be viewed (either directly by contacting the running service, or indirectly via an intermediary) and updated
- **Enforcement**
  - Policies are verified and enforced by the ESB.
- **Storage**
  - A library of policy types can be built up and shared between services and developers

Policy Management



Policy Enforcement



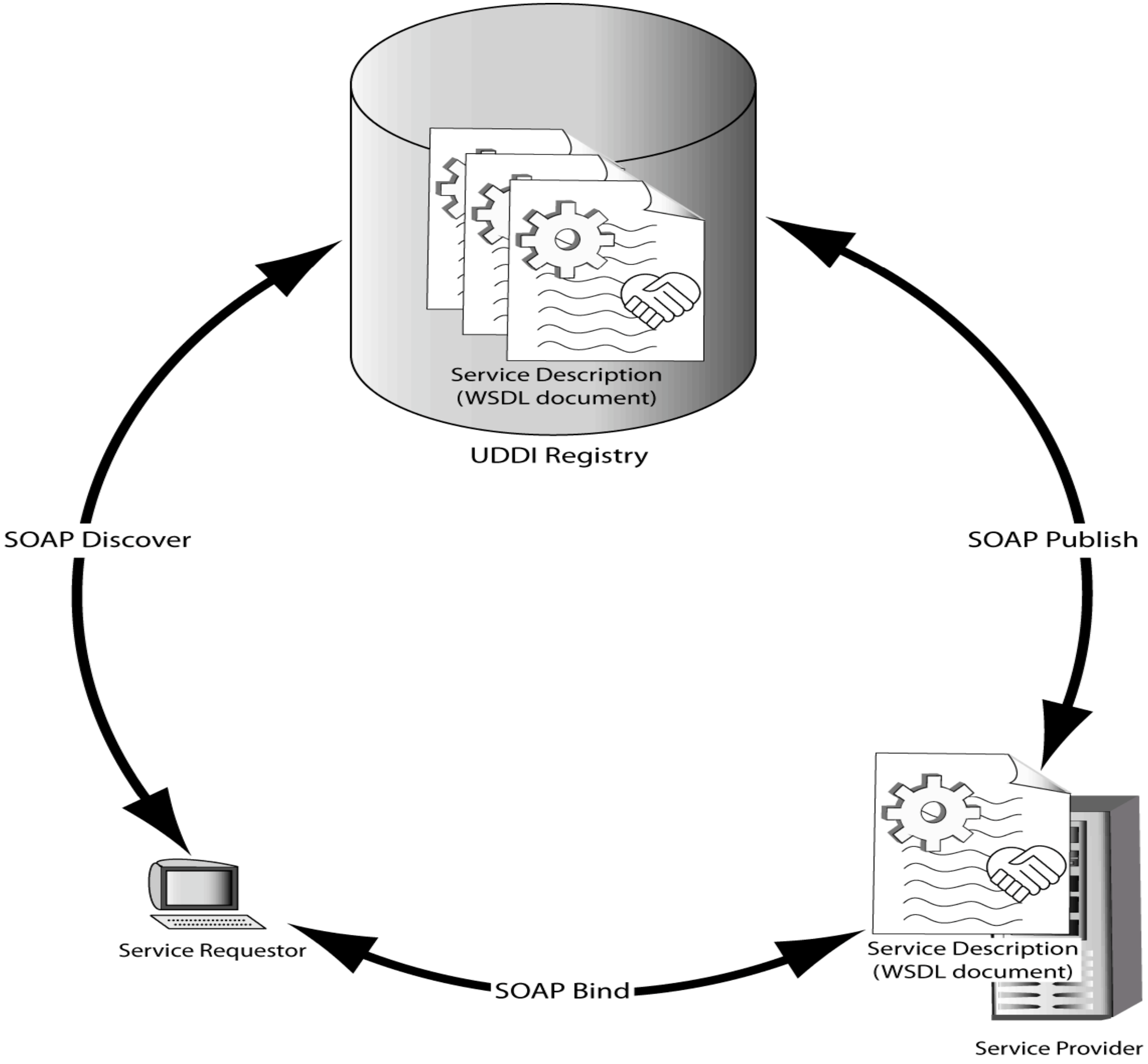
Other meta-data

- Policies that describe configuration/description information for non-functional capabilities of the service, such as those defined by the WS-Security or WS-TX policies, for configuring low-level security and transactional aspects of the service.
- Policies that are markers for compliance or compatibility with certain standards or specifications, such as support for WS-Addressing or compliance with the WS-I basic profiles.
- Policies that represent constraints that must be fulfilled, such as SLAs or contractual obligations.

The component triad

- **Provider**
  - A provider is an entity that makes a Service available for use by one or more Requestors, optionally facilitating this by publishing details of the Service through a Broker
- **Requestor**
  - A requestor is an entity that uses (consumes) a Service. It may discover the availability and details of this Service via. a Broker or by other means
- **Broker**
  - A broker is an entity that provides directory style registration and lookup service to Providers and potential Requestors
    - Registry and repository

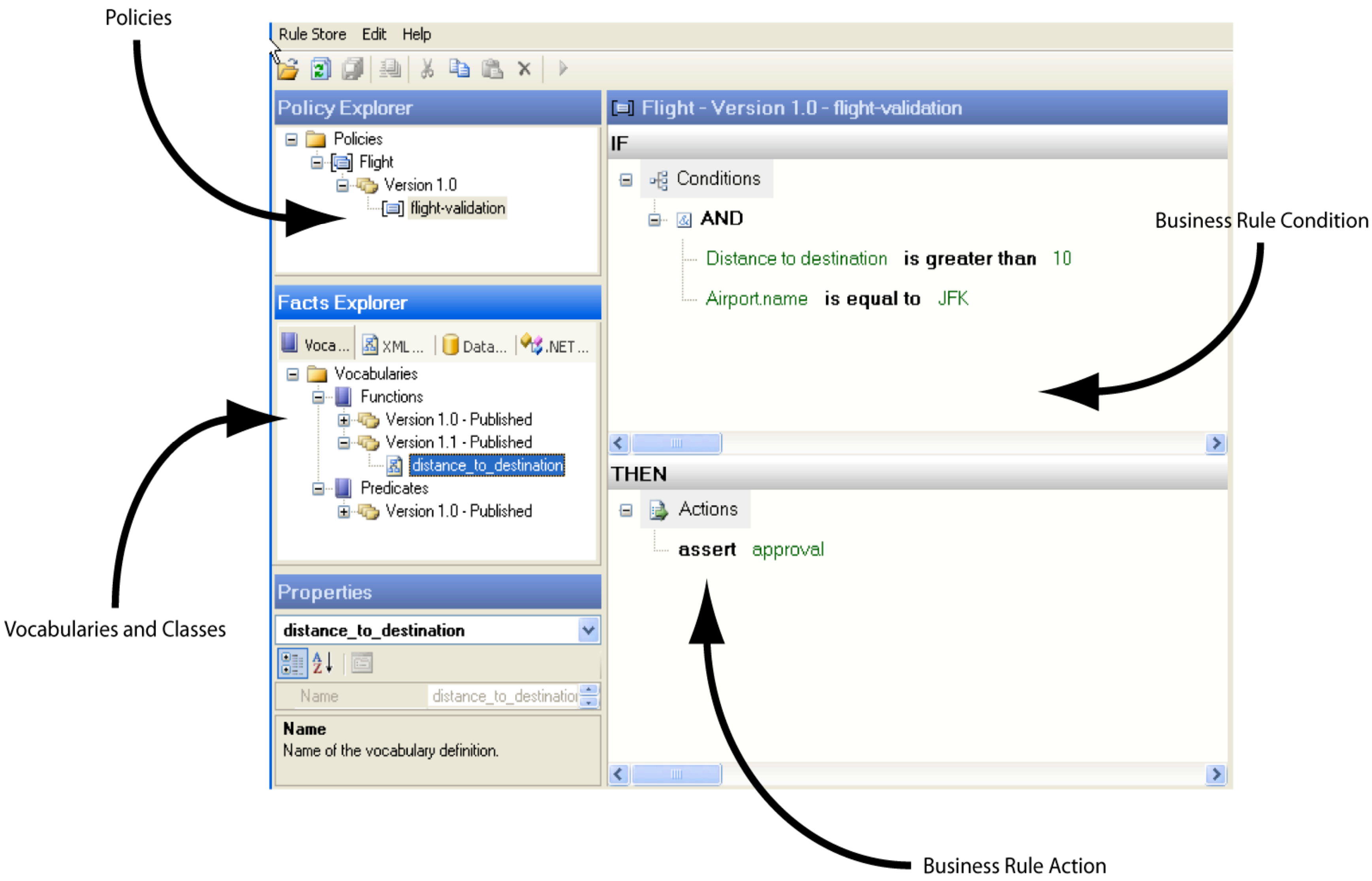
Web Services implementation



Repository

- **Service metadata, which is important for contract definitions**
  - Functional and non-functional aspects
    - Transactional, secure, QoS, …
    - Policies
  - MEPs
    - One-way
    - Request-response
  - Message structure
    - Where data resides
  - Governance
- **Service binaries**
- **Business rules**
- **Workflow tasks or process control information**

The BRMS



Policy Explorer

- Policies
  - Flight
    - Version 1.0
      - flight-validation

Facts Explorer

- Vocabularies
  - Functions
    - Version 1.0 - Published
    - Version 1.1 - Published
      - distance_to_destination
  - Predicates
    - Version 1.0 - Published

Properties

distance_to_destination

Name	distance_to_destinatioi

Name
Name of the vocabulary definition.

Flight - Version 1.0 - flight-validation

IF

- Conditions
  - AND
    - Distance to destination **is greater than** 10
    - Airport.name **is equal to** JFK

THEN

- Actions
  - **assert** approval

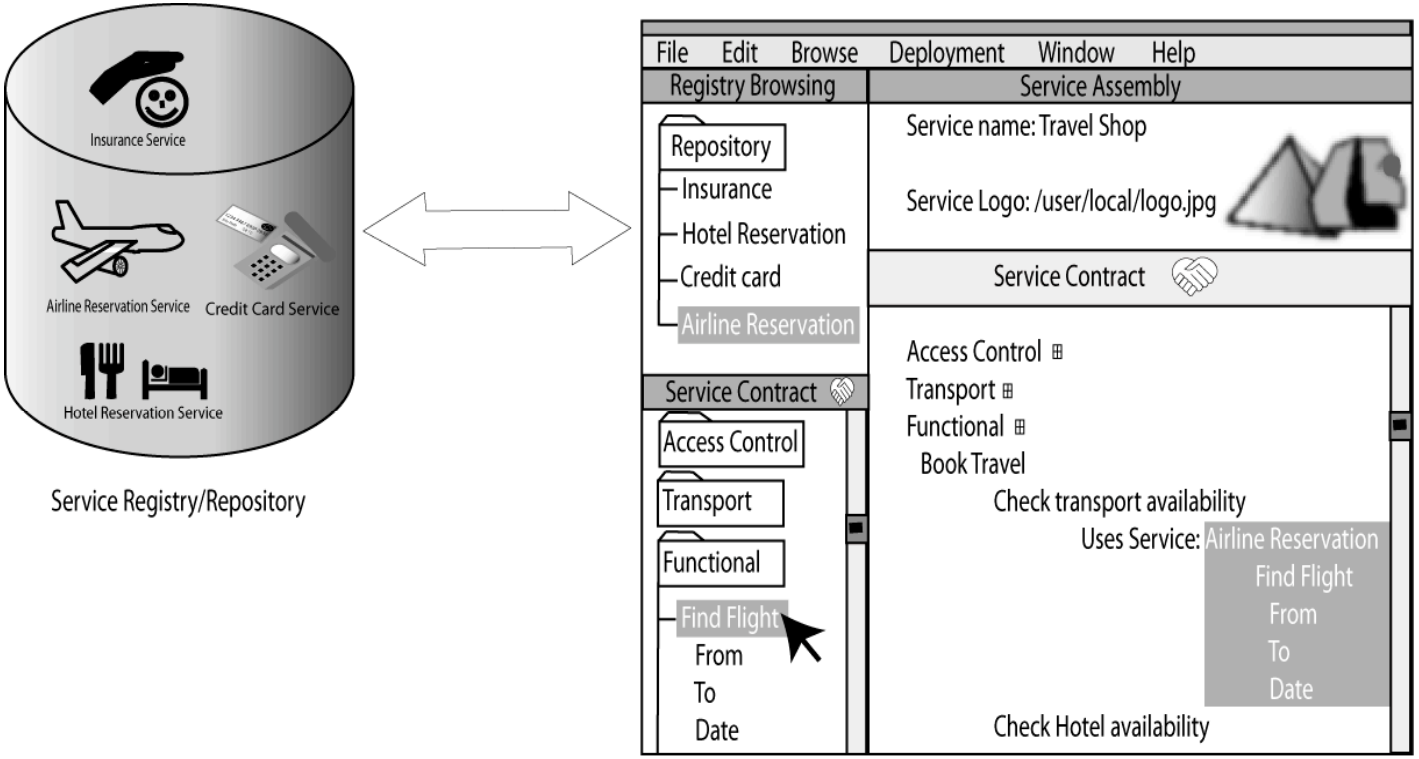
Policies

Vocabularies and Classes

Business Rule Condition

Business Rule Action

Design-time service discovery



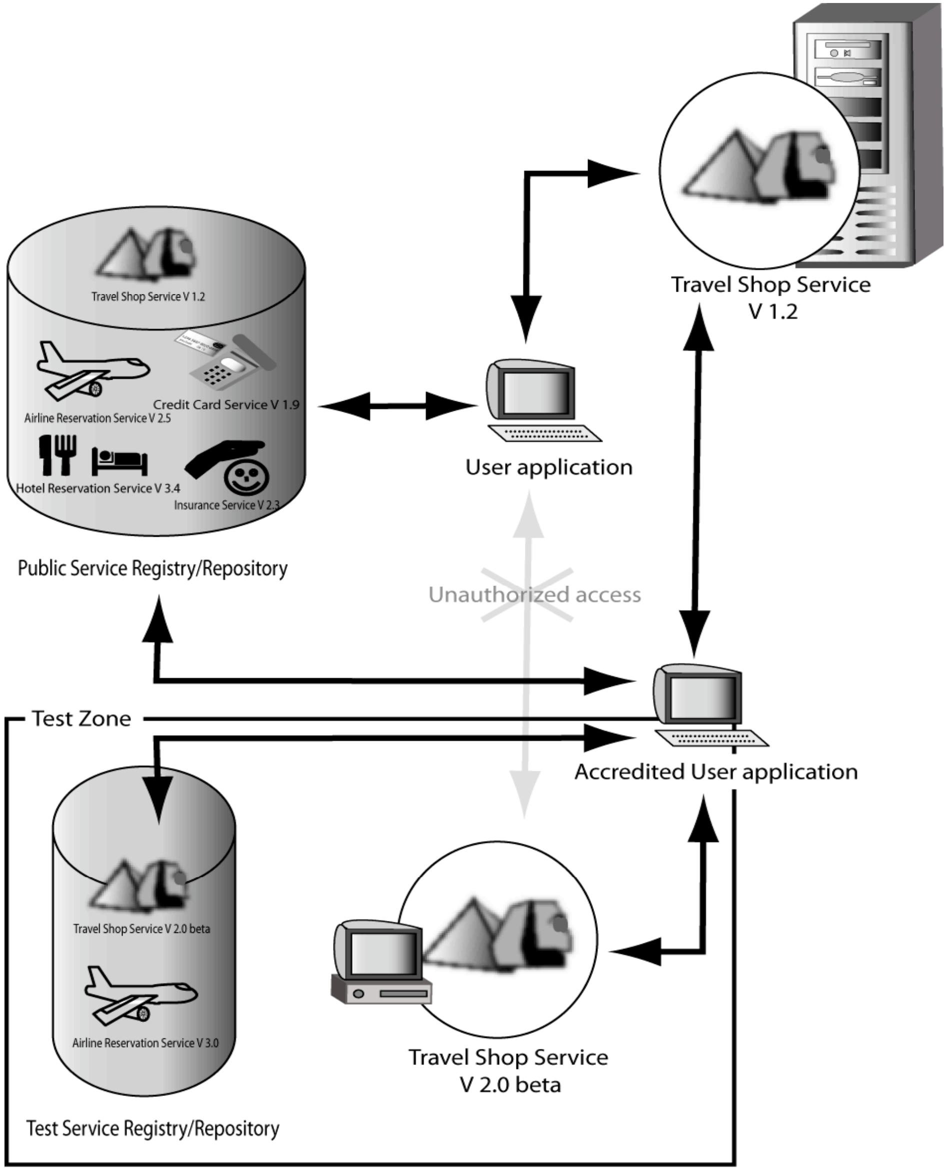
Service name: Travel Shop

Service Logo: /user/local/logo.jpg

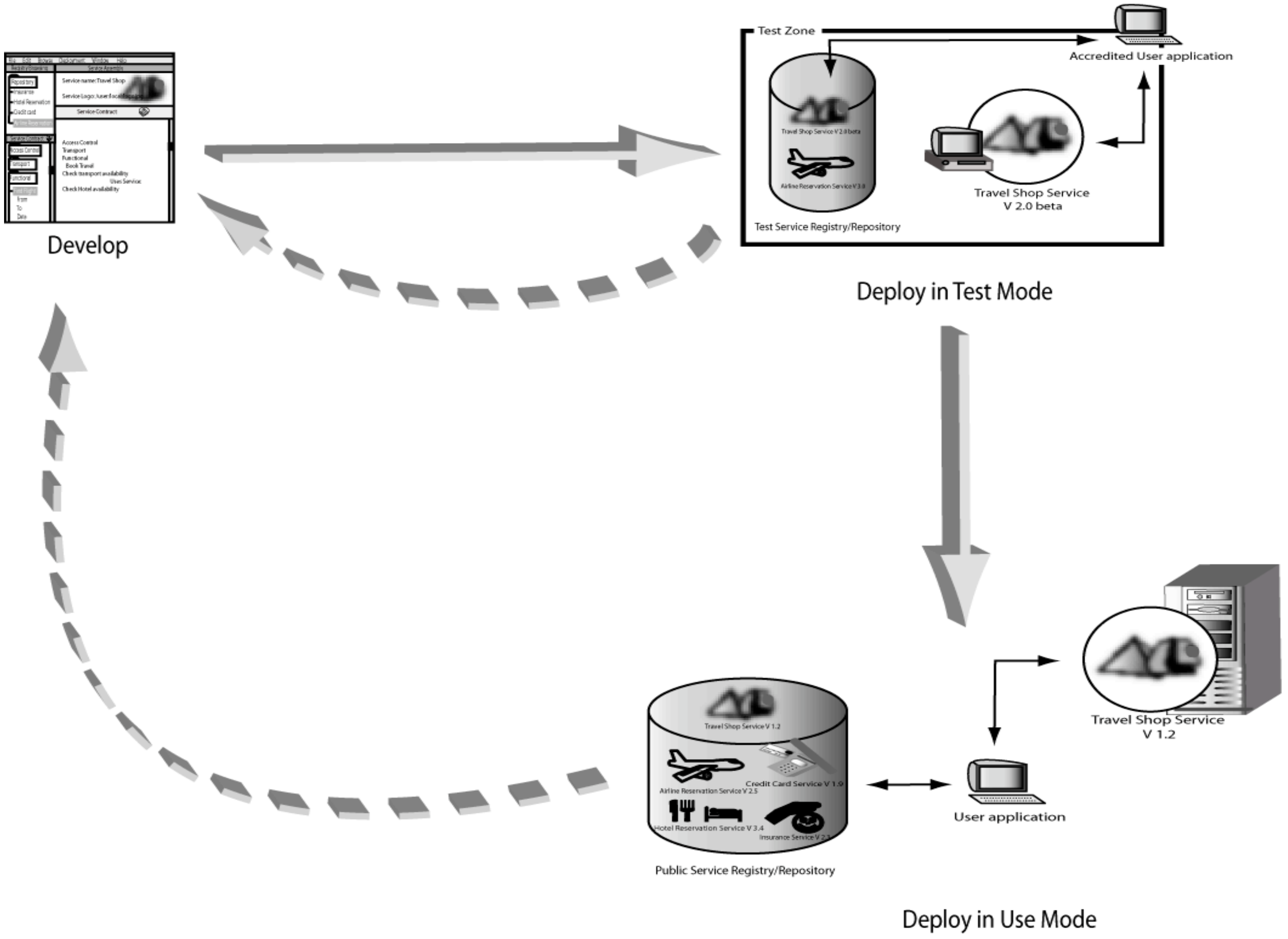
Service Contract

Access Control ⊞
Transport ⊞
Functional ⊞
Book Travel
Check transport availability
Uses Service: Airline Reservation
Find Flight
From
To
Date
Check Hotel availability

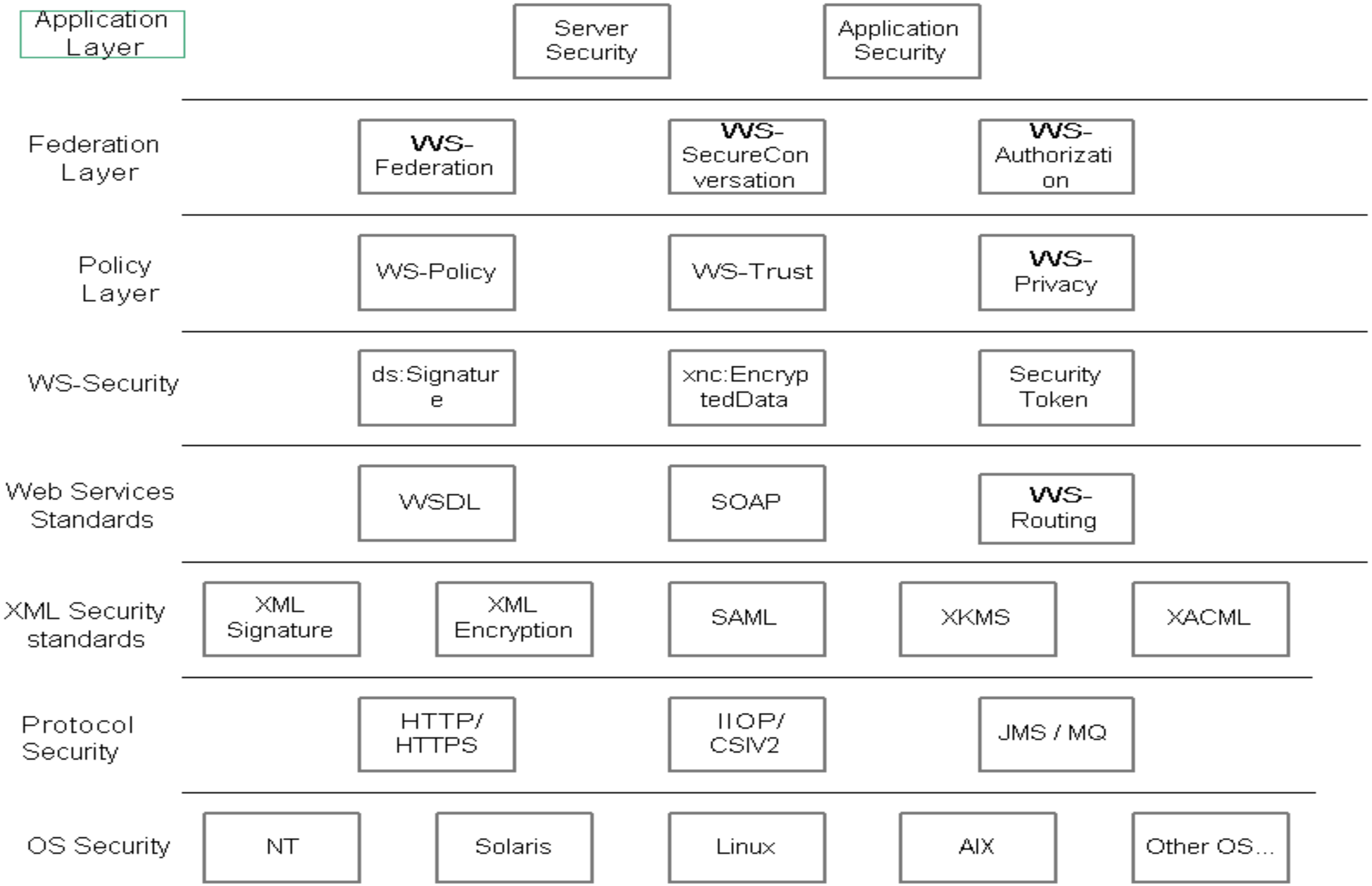
Service testing


Travel Shop Service V 1.2
Airline Reservation Service V 2.5
Credit Card Service V 1.9
Hotel Reservation Service V 3.4
Insurance Service V 2.3
Public Service Registry/Repository
User application
Travel Shop Service
V 1.2
Unauthorized access
Test Zone
Accredited User application
Travel Shop Service V 2.0 beta
Airline Reservation Service V 3.0
Test Service Registry/Repository
Travel Shop Service
V 2.0 beta

Service deployment



Security



Application Layer: Server Security, Application Security

Federation Layer: WS-Federation, WS-SecureConversation, WS-Authorization

Policy Layer: WS-Policy, WS-Trust, WS-Privacy

WS-Security: ds:Signature, xnc:EncryptedData, Security Token

Web Services Standards: WSDL, SOAP, WS-Routing

XML Security standards: XML Signature, XML Encryption, SAML, XKMS, XACML

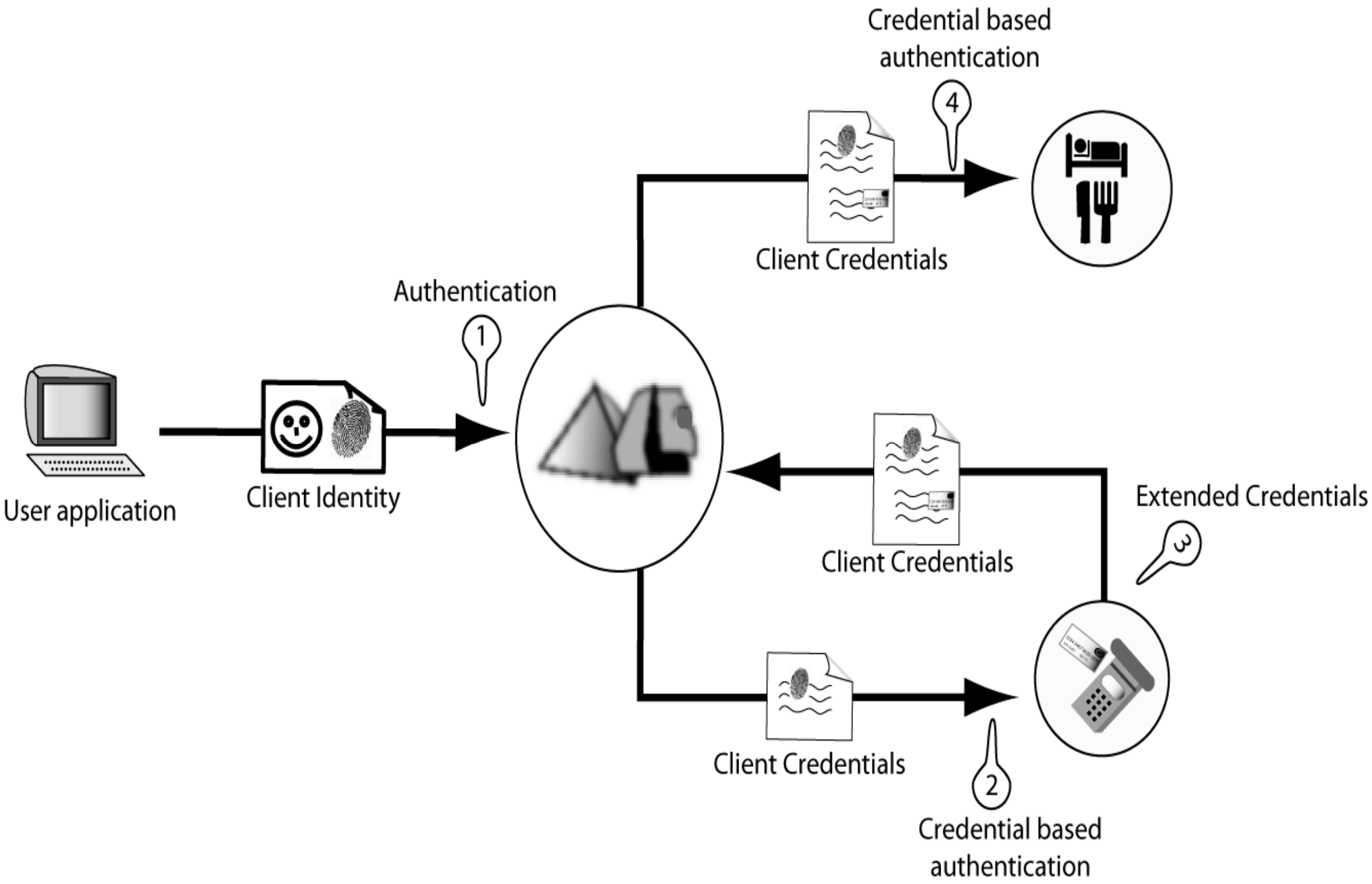
Protocol Security: HTTP/ HTTPS, IIOP/ CSIV2, JMS / MQ

OS Security: NT, Solaris, Linux, AIX, Other OS...

Identity within SOA

- Must have some means by which a user (human or process) can establish its identity (obtain a credential) and then pass this to a target service in a format it understands
  - **Standards based formats are very important**
    - **WS-Security**
- It is common to have composite services forming a hierarchy
  - **The SOA must ensure that every intermediary can authenticate the requesting client (which could be a service) before passing credentials to the next service**
  - **As the credential information flows, it may be augmented or completely changed by each intermediate service: identity management must be federated hierarchically in order for it to scale and match the business domain**

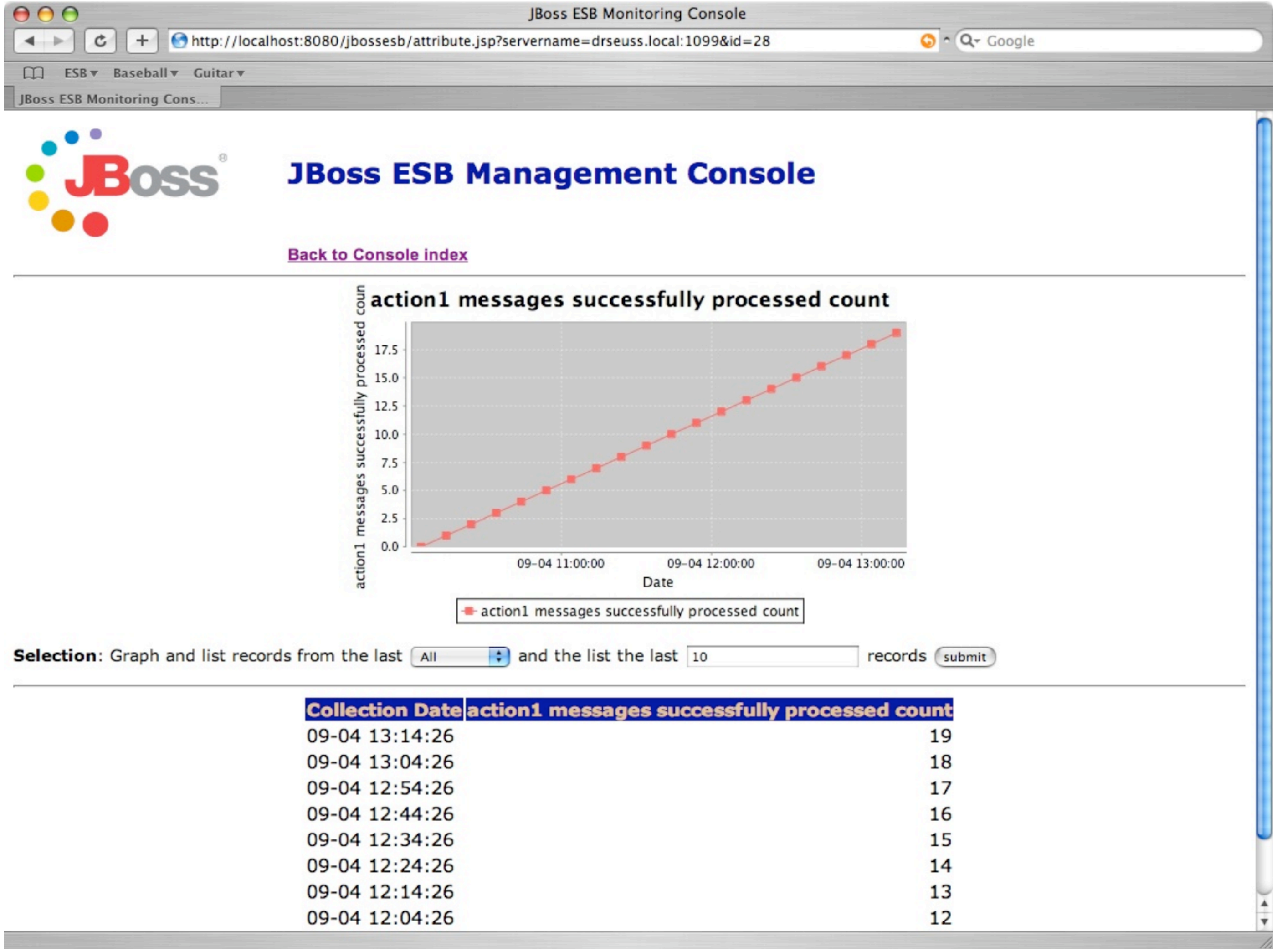
Identity management



Business Activity Monitoring

- Real-time access to critical business performance metrics
  - **Helps to improve the efficiency and effectiveness of business processes**
- Real-time process/service monitoring is a common capability supported in many distributed infrastructures
  - **BAM differs in that it draws information from multiple sources to enable a broader and richer view of business activities**
  - **BAM also encompasses business intelligence as well as network and systems management**
  - **BAM is often weighted toward the business side of the enterprise**
    - **As such, there has recently been a movement for good BAM implementations to be closely related to the governance infrastructures**

BAM


JBoss ESB Monitoring Console
http://localhost:8080/jbossesb/attribute.jsp?servername=drseuss.local:1099&id=28
Google
ESB ▾
Baseball ▾
Guitar ▾
JBoss ESB Monitoring Cons...
action1 messages successfully processed coun
17.5
15.0
12.5
10.0
7.5
5.0
2.5
0.0
09-04 11:00:00
09-04 12:00:00
09-04 13:00:00
Date
action1 messages successfully processed count

JBoss ESB Management Console

Back to Console index

action1 messages successfully processed count

Selection: Graph and list records from the last All and the list the last 10 records submit

Collection Date	action1 messages successfully processed count
09-04 13:14:26	19
09-04 13:04:26	18
09-04 12:54:26	17
09-04 12:44:26	16
09-04 12:34:26	15
09-04 12:24:26	14
09-04 12:14:26	13
09-04 12:04:26	12