An Architecture for Integrating Security across CORBA, J2EE and Web Services

Quadrāsis™

Ted Burghart

Ted.Burghart@Quadrasis.com

Hitachi Computer Products (America), Inc.

Introduction

- With the rapid pace of product development focused on Web Services and the abundance of security technologies being deployed throughout the enterprise, integration of these disparate products and services becomes increasingly important in order to maintain a manageable level of complexity.

Administrators, unable to manage the incompatible security technologies in any other way, resort to replication of data and effort across multiple security datastores.

Auditors are unable to establish the trustworthiness of the complete system.

Quadrāsis™

Security Fundamentals

- Authentication
  - Proving the principal's identity
  - Multi-factor authentication
- Authorization
  - Controlling access to protected resources
- Accountability
  - Who got access to what, when
  - Why - how the decision was made
- Availability
  - Rejection of attacks
  - Access to authorized clients assured

Quadrāsis™

System Requirements

- Administration
  - Common control point for most, if not all, policies
- Availability
  - Failover
  - Redundancy
  - Fault tolerance
- Scalability
  - Statefull or stateless?
- Standards Support
  - JCP
  - OASIS
  - OMG
  - W3C
  - The Next Big Thing ™

Quadrāsis™

Platform Requirements

- Middleware
  - COM
  - CORBA
  - J2EE
  - Web Services
- Operating System
  - Unix
  - Windows
- Programming Language
  - C++
  - C#
  - Java

Quadrasis™

What do they have in common?

- Authentication
  - Translate evidence to credentials
  - Attributes
    - Translate credentials to privileges
- Authorization
  - Push vs. Pull
  - Granularity
- Is that it?
  - If it were only that simple …

Quadrāsis™

How do they differ …

- Authorization
  - Push vs. Pull
  - Granularity
    - Users
    - Groups
    - Roles
    - Privileges
    - Realms
    - Servers
    - Objects
    - Methods
    - Domains
    - Transports
    - Directories
    - Files
- Attribute Services
  - Translate some input to some output
- Accountability ?
- Administration ?
- Availability ?

Quadrāsis™

… and what can we do about it?

- Mapping
  - Credentials
  - Attributes
  - Decisions
  - Auditable events?
- Correlation
  - Event stream
- Policy
  - Is it even possible?
  - Ok, is it feasible?

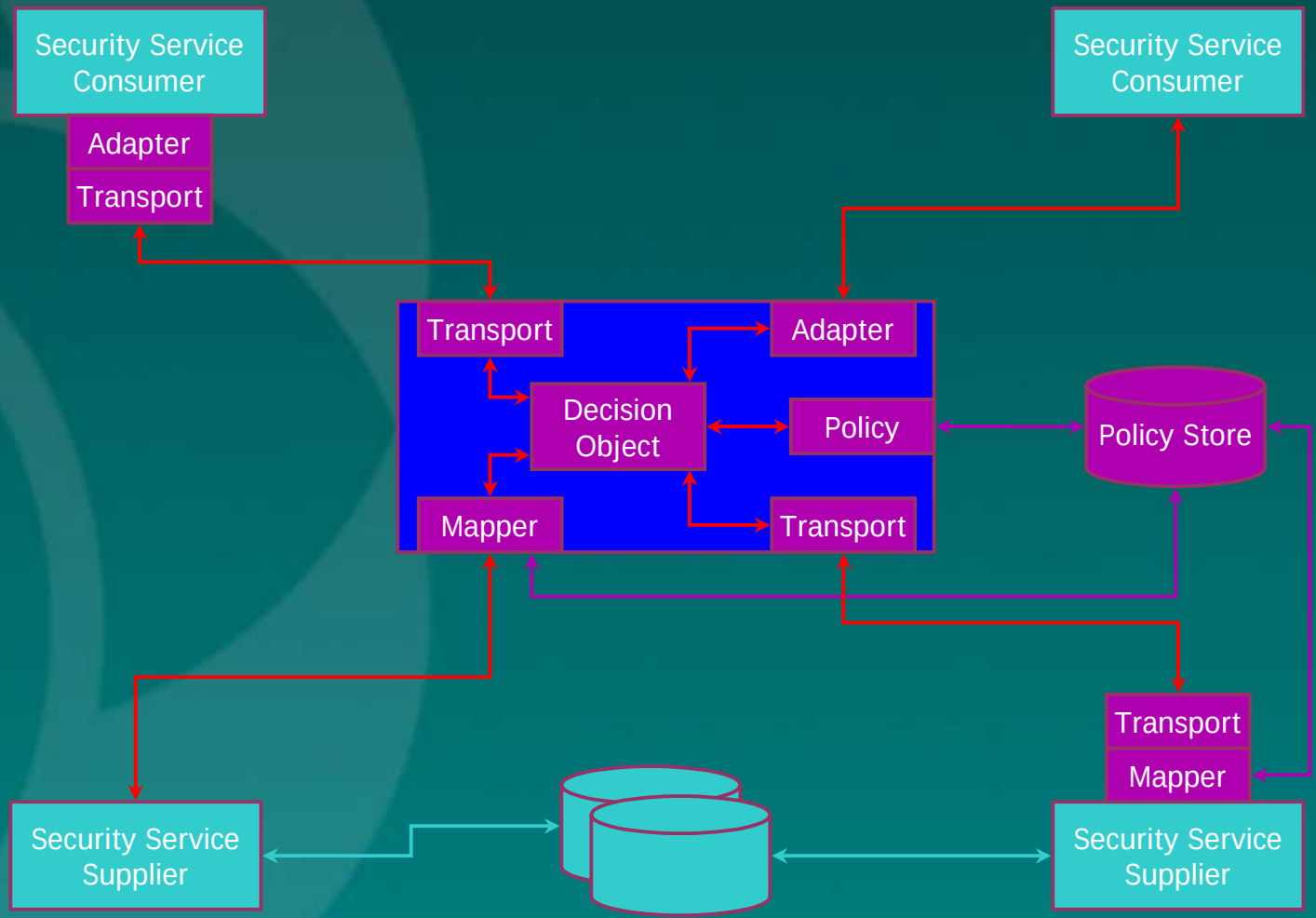
Quadrāsis™

QPiK Plugin Architecture

- Loadable Services
  - Adapters
  - Mapping
  - Reporting
  - Routing
  - Translation
  - Transport
- Configuration
  - Transparency
  - Dependencies

Quadrāsis™

EASI Architecture

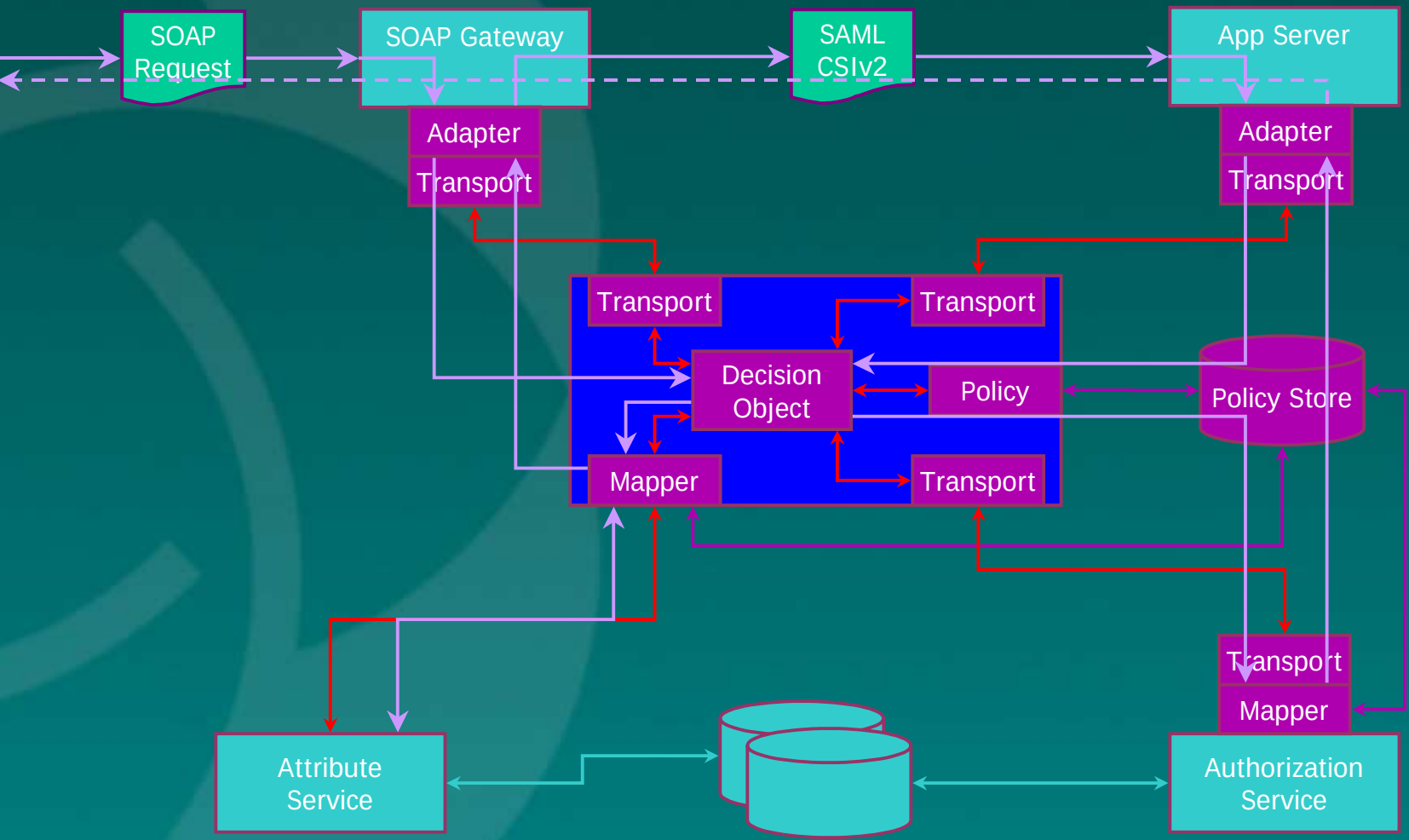


Trusting the trust decision

- Can we trust it when we're done?
  - Consolidated configuration
  - Secure transport
  - DSIGs on messages
- But …
  - Can't trust anything more than the least-trusted component
    - In many cases, that's the transport layer!
    - Where's the private key for *your* SSL server?
    - Where's the key encryption key for your private key?
  - DSIGs on decision modules
    - And where do the keys for that come from?

Quadrasis™

Deployment Scenario



Quadrasis™