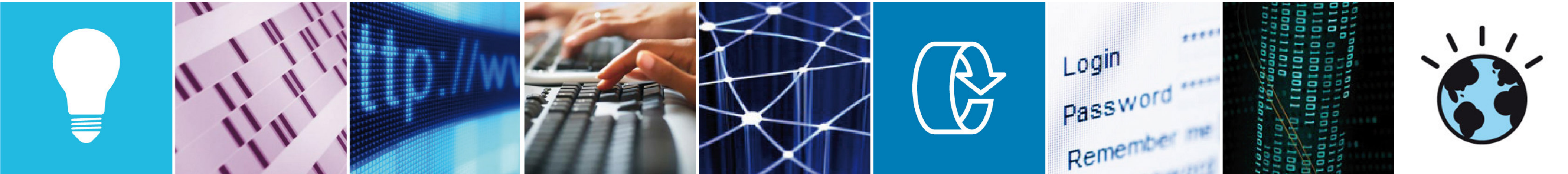
SOA ARCHITECT SUMMIT

Turn your ideas into practical solutions.

How to tackle Security in a SOA world?

Martin Borrett
Lead Security Architect NE Europe, WW Tivoli Tiger Team



Abstract

- **In this session I will highlight the progress that our clients have made in understand the security challenges of SOA. Secondly I will discuss the technology and standards available today to solve these issues. Finally I will share successful customer examples of bringing these two aspects together to deliver business value and mitigate these risks.**

Agenda

- **SOA Security Considerations**
- **SOA Entry Points and Security**
- **SOA Security Architecture Approaches**
- **Security Standards**
- **Technology and solutions**
  - TFIM
  - TSPM
- **Customer Case studies**

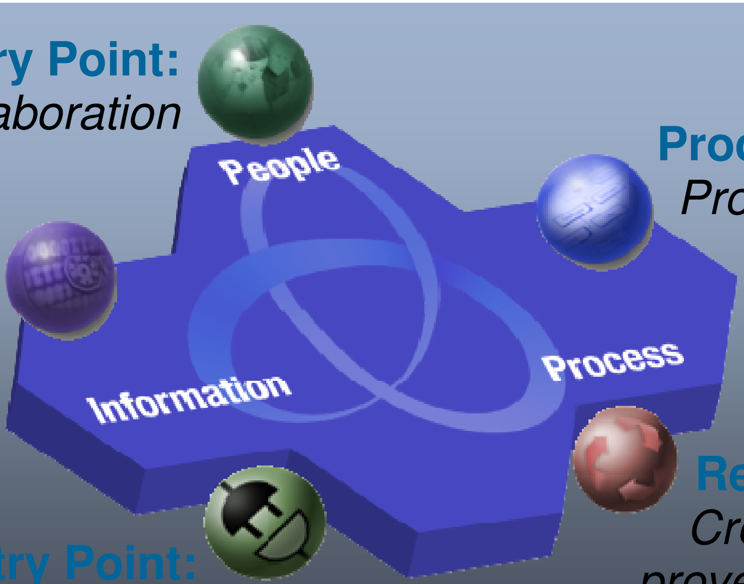
Security Considerations for SOA

- **Organizational/enterprise boundaries**
  - Perimeter is obscure
  - Identities are managed across boundaries
  - Trust relationships are established across boundaries
- **Composite applications**
  - Ensuring proper security controls are enacted for each service and when used in combination
- **Entities/Identities – users, services**
  - Services have identities
  - Identities and/or credentials are propagated across services
  - Users and services are now subject to the same security controls
- **Greater focus on data/information**
  - Protecting data at transit and at rest
  - Apply consistent protection measures
  - Access to data by applications and services
- **Governance, Risk, and Compliance**
  - Auditing ie. entity identification to specific transactions

The SOA Entry Points

- *When selecting SOA projects, focus on solving **specific business problems** as part of an evolving enterprise architecture*

- *IBM has a variety of assets and best practices around the SOA entry points, based on our **extensive experience with customers***



People Entry Point:
Interaction and Collaboration

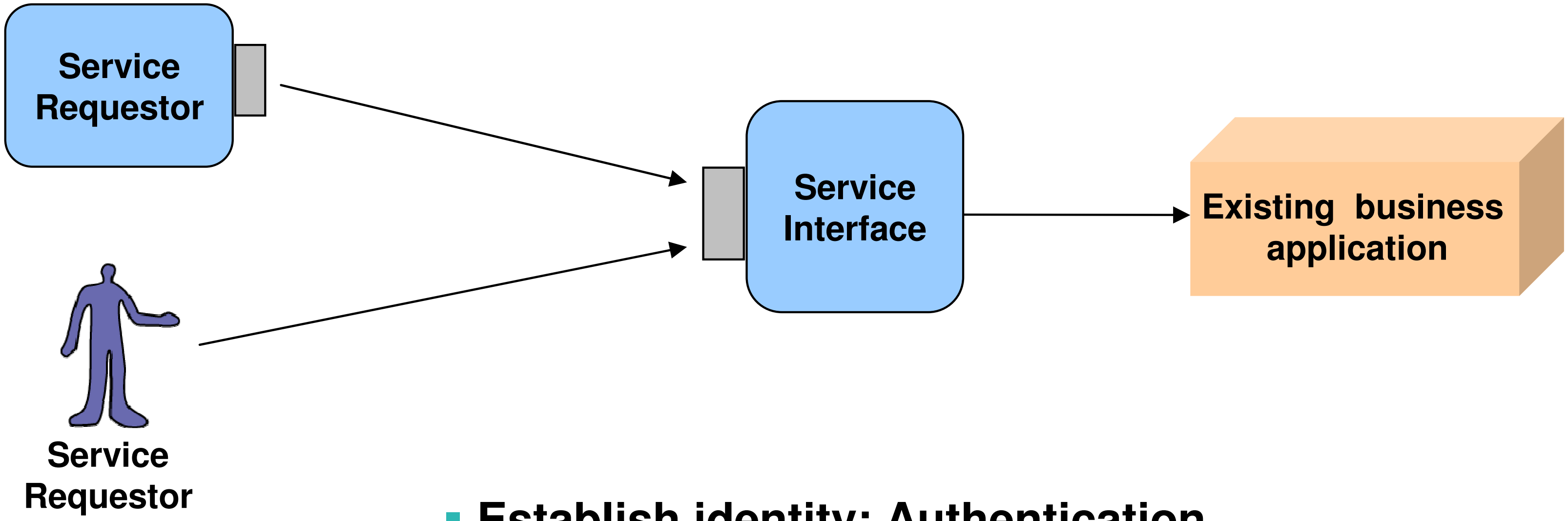
Process Entry Point:
Process Automation

Information Entry Point:
Information as a Service

Reuse Entry Point:
Creating and reusing proven, high-value assets

Connectivity Entry Point:
Securely and flexibly interconnecting

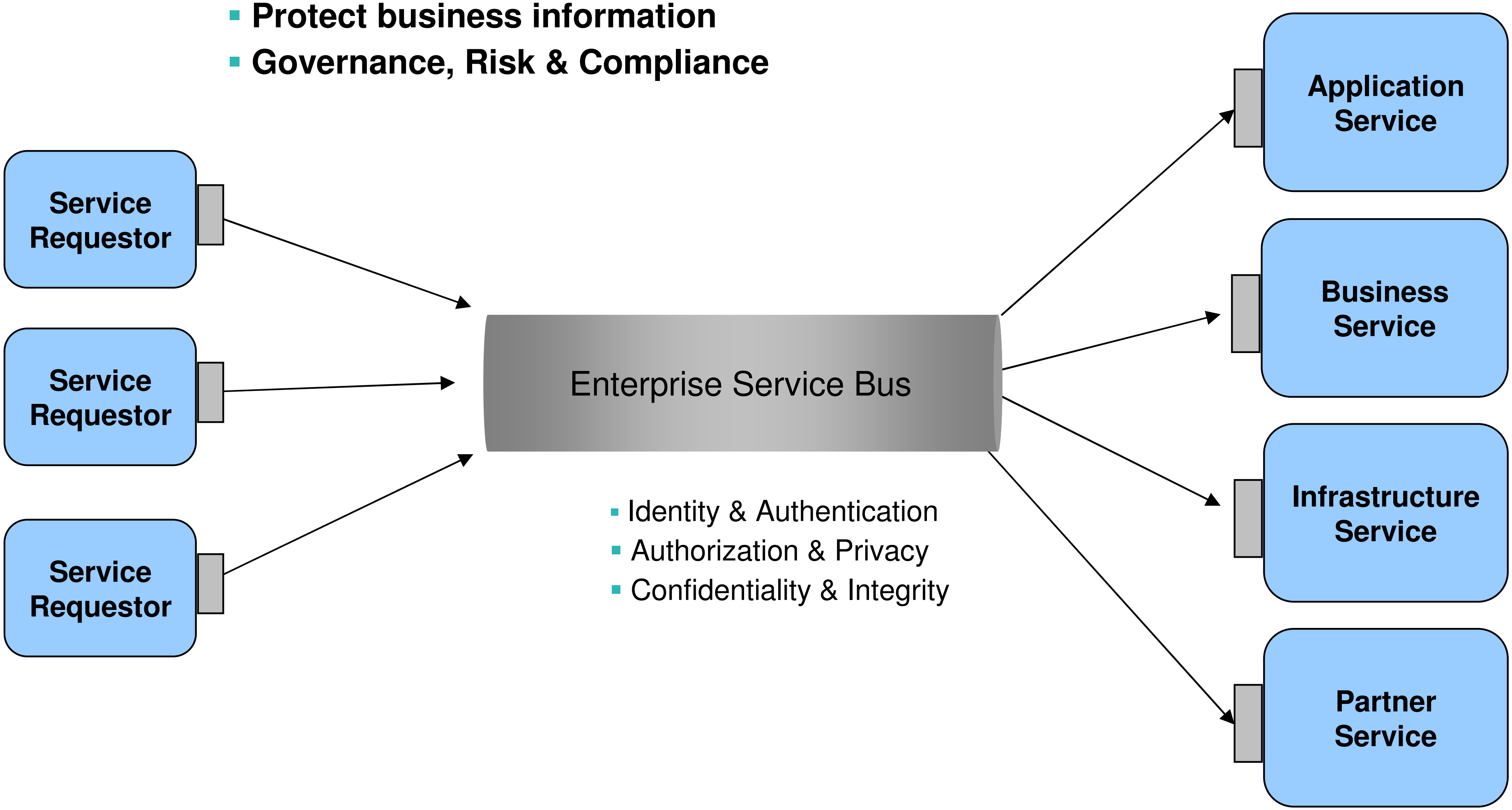
Reuse - Service Creation



- Establish identity: Authentication
- Protect messages: Confidentiality & Integrity
- Accountability: Audit access to service
- User experience: SSO, Privacy

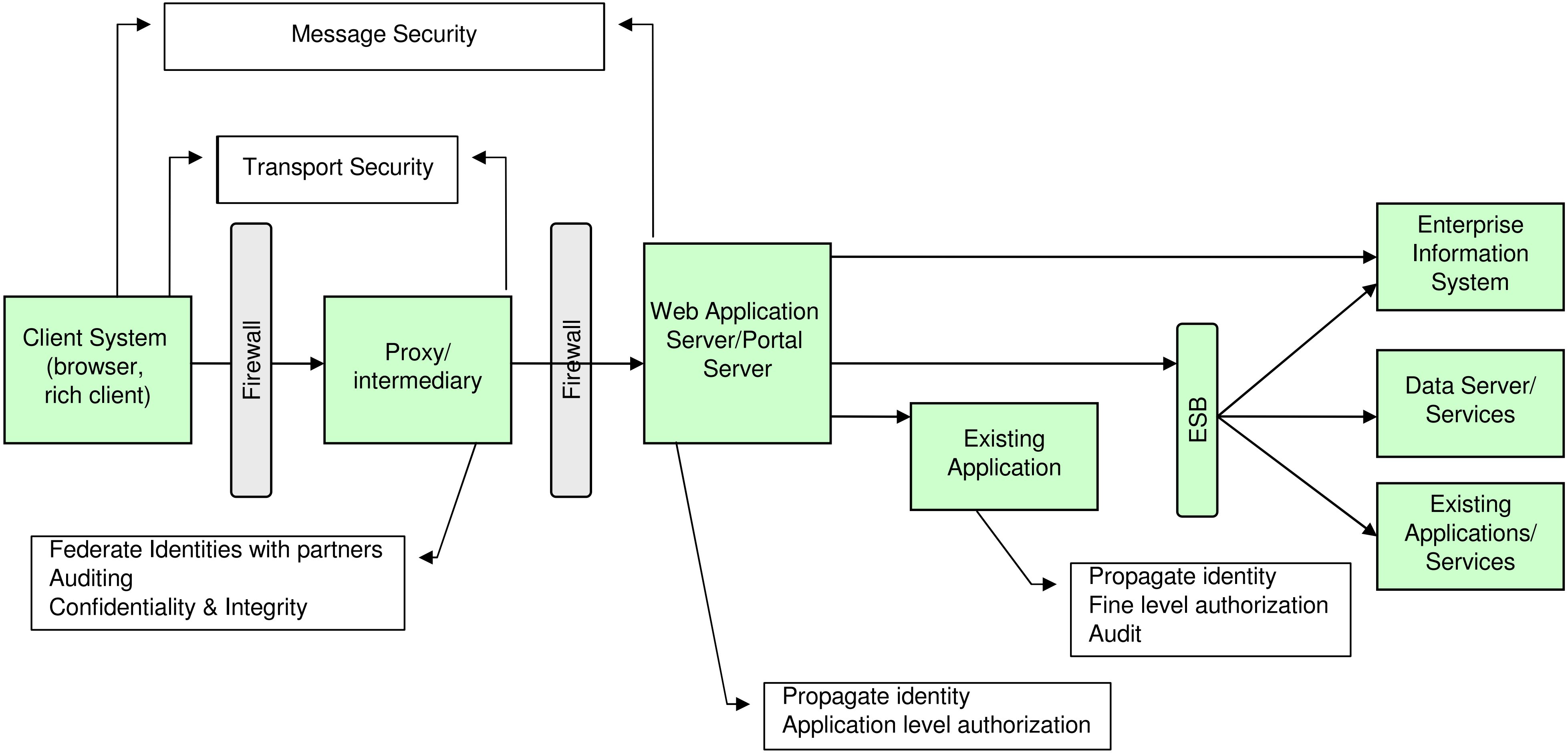
Connectivity - Service Integration

- Propagate identity: Cross domain/realm identity mapping and token transformation
- Reflect business relationships: Trust Management (for data, identity, etc)
- Protect business information
- Governance, Risk & Compliance

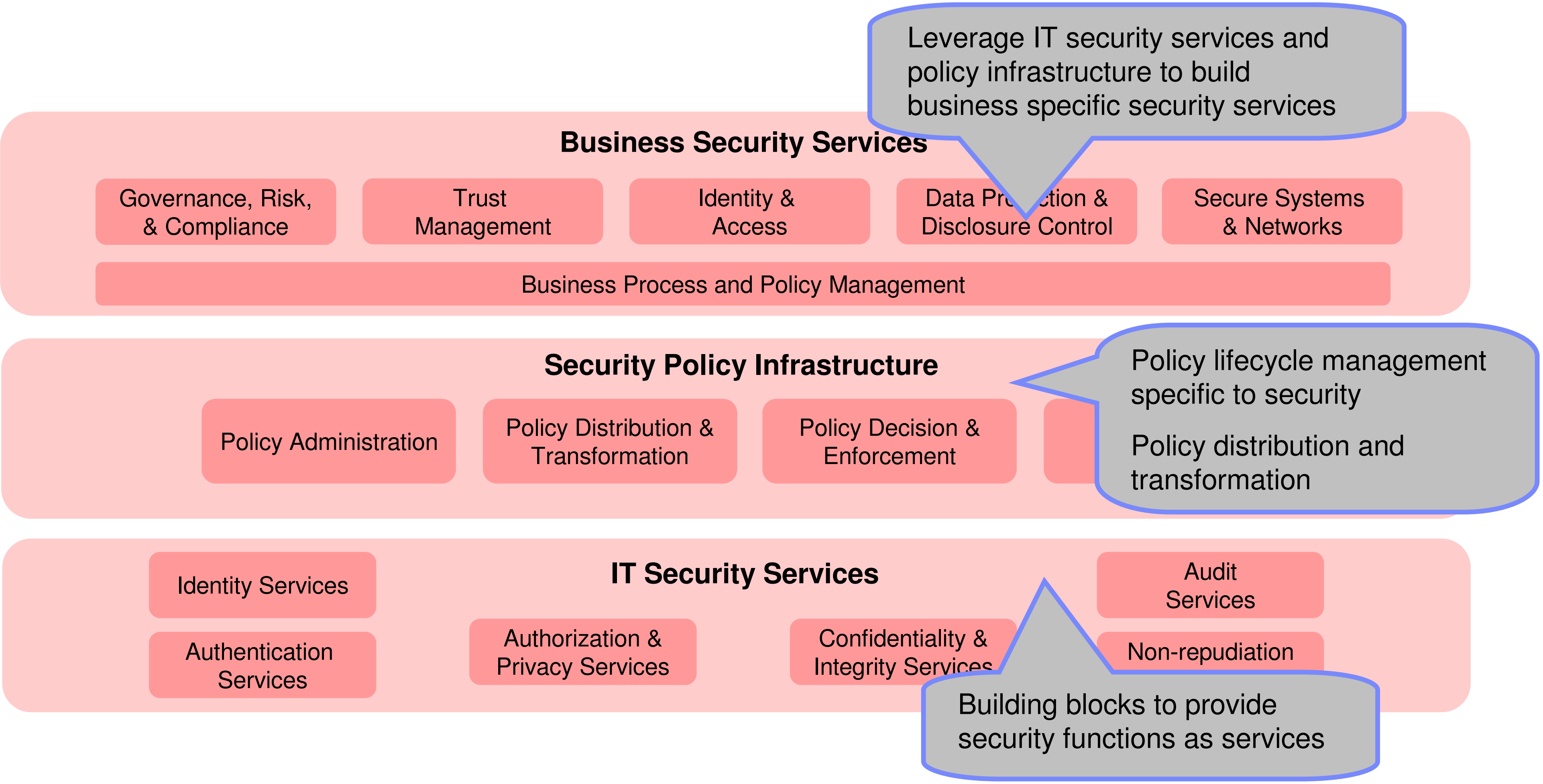


- Identity & Authentication
- Authorization & Privacy
- Confidentiality & Integrity

Security in a Typical Deployment Architecture


Message Security
Transport Security
Client System (browser, rich client)
Firewall
Proxy/ intermediary
Firewall
Web Application Server/Portal Server
Enterprise Information System
ESB
Data Server/ Services
Existing Application
Existing Applications/ Services
Federate Identities with partners
Auditing
Confidentiality & Integrity
Propagate identity
Fine level authorization
Audit
Propagate identity
Application level authorization

SOA Security – Reference Model



Leverage IT security services and policy infrastructure to build business specific security services

Business Security Services

Governance, Risk, & Compliance

Trust Management

Identity & Access

Data Pro ction & Disclosure Control

Secure Systems & Networks

Business Process and Policy Management

Security Policy Infrastructure

Policy Administration

Policy Distribution & Transformation

Policy Decision & Enforcement

Policy lifecycle management specific to security

Policy distribution and transformation

IT Security Services

Identity Services

Authentication Services

Authorization & Privacy Services

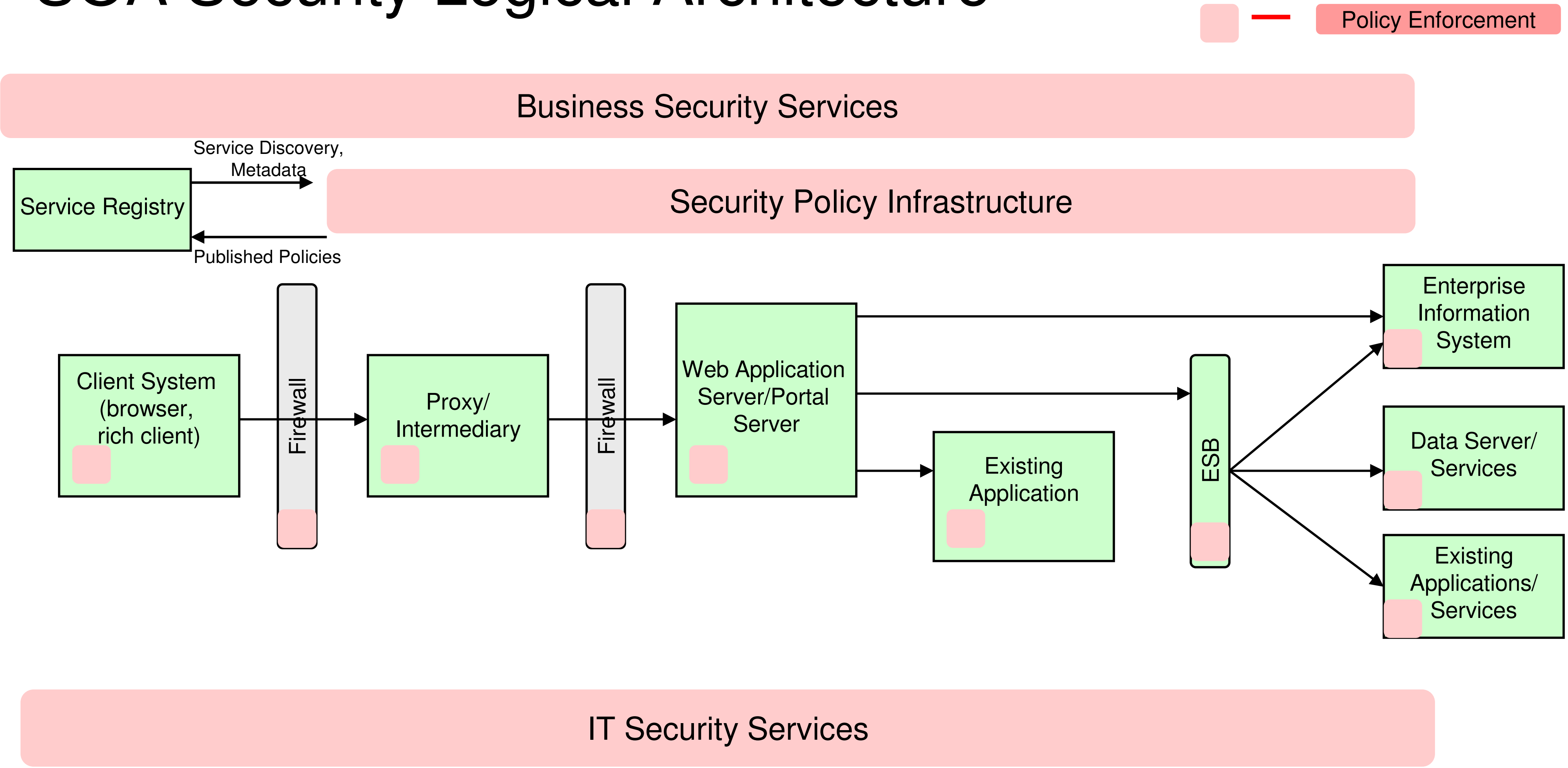
Confidentiality & Integrity Services

Audit Services

Non-repudiation

Building blocks to provide security functions as services

SOA Security Logical Architecture

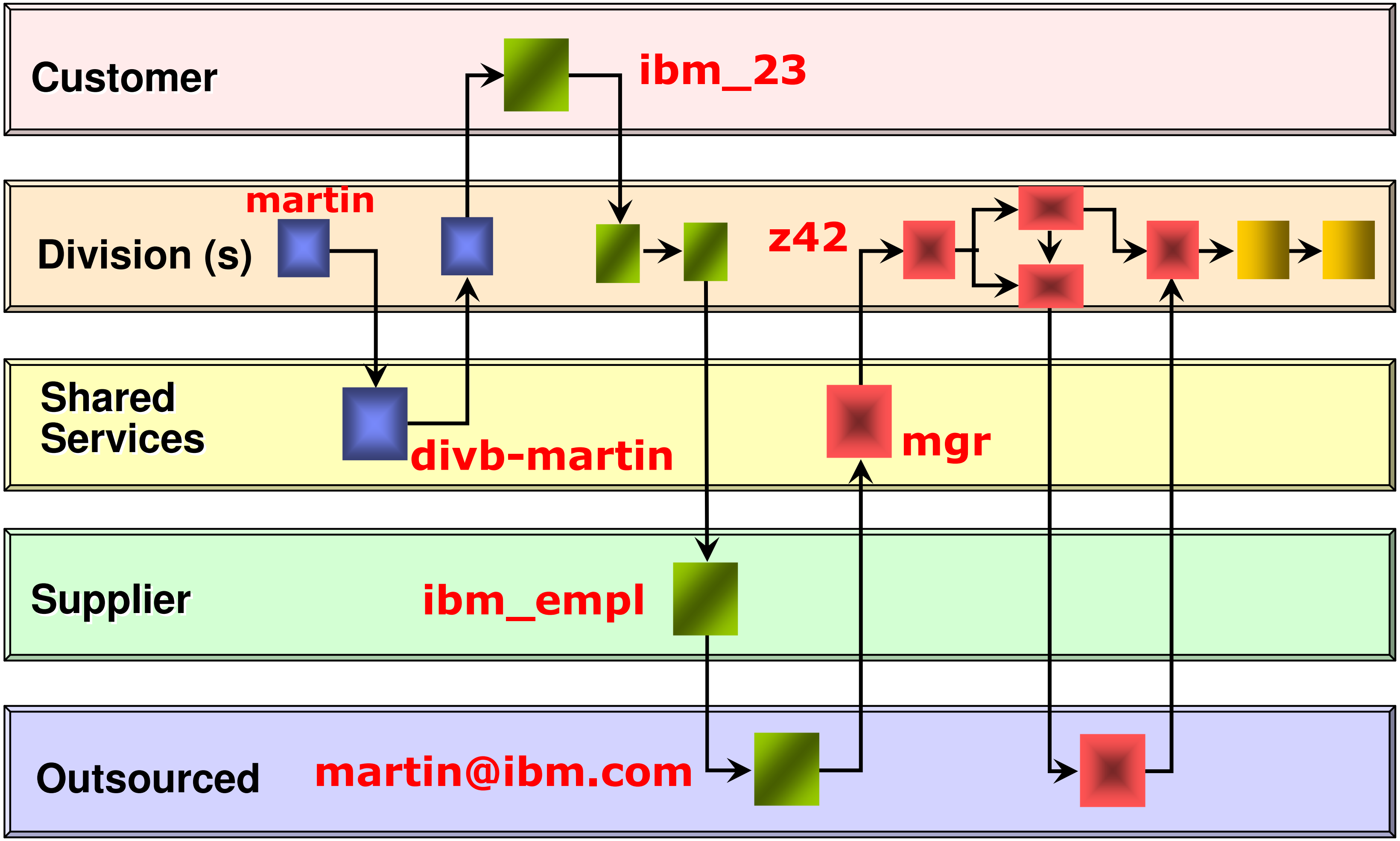

🟥 — Policy Enforcement
Business Security Services
Service Registry
Service Discovery, Metadata
Published Policies
Security Policy Infrastructure
Client System (browser, rich client)
Firewall
Proxy/ Intermediary
Firewall
Web Application Server/Portal Server
Existing Application
ESB
Enterprise Information System
Data Server/ Services
Existing Applications/ Services
IT Security Services

Policies are distributed to not only to Security Services but only to different enforcement points.

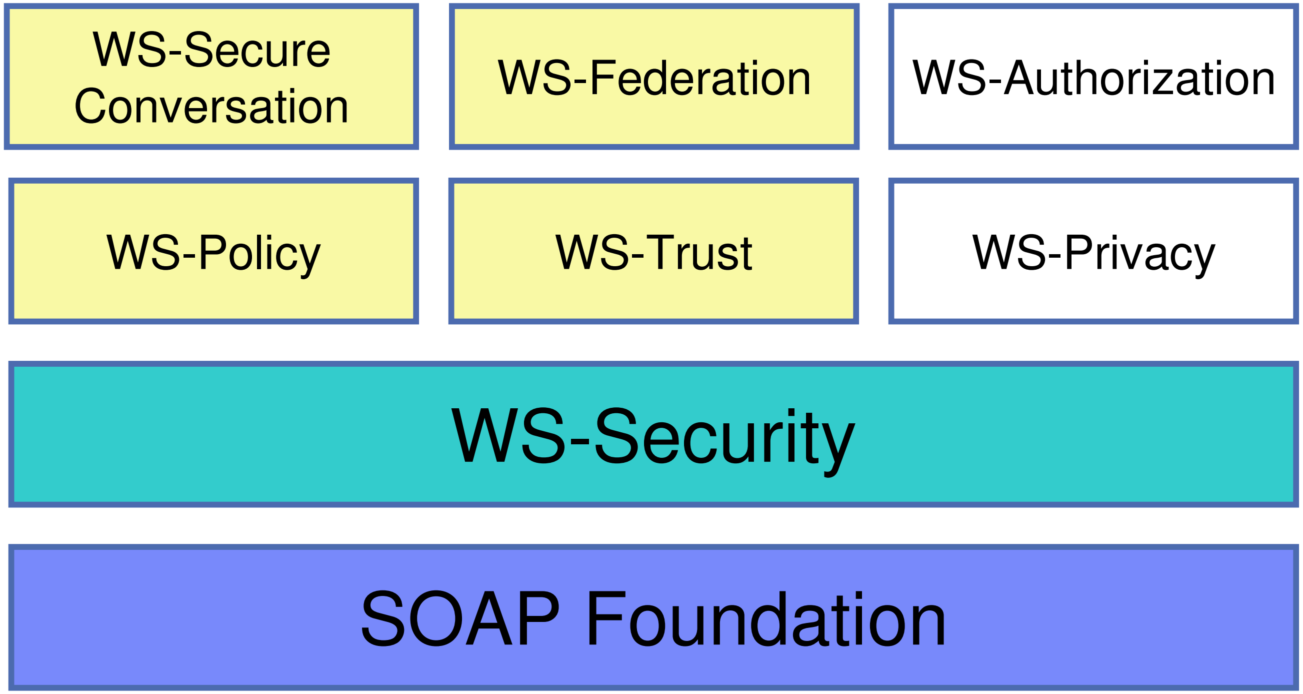
The Enforcement points can leverage local capabilities or access centralized security services to enforce policies.

Identity Flow in a Service Oriented Architecture

How does Identity flow between services ?



Web Services Security Roadmap



WS-Secure Conversation

WS-Federation

WS-Authorization

WS-Policy

WS-Trust

WS-Privacy

WS-Security

SOAP Foundation

Web services zone page:
http://www-106.ibm.com/developerworks/webservices/

WS-Security : SOAP Message Security

- **WS-Security : SOAP Message Security**
  - defines "…a standard set of SOAP extensions that can be used when building secure Web services to implement integrity and confidentiality."

- **Allows:**
  - sending Security Tokens to authenticate requests
  - signing Data to ensure data integrity and verify sender
  - encrypting Data to ensure privacy of data

- **Goal:**
  - "End-to-end message content security…"

WS-Trust : Overview

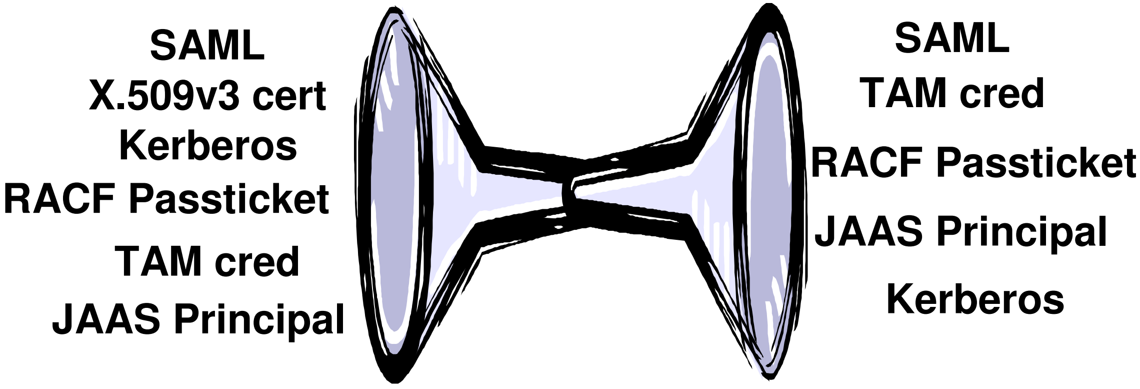
- **WS-Trust defines mechanism for:**
  - "…security token exchange to enable the issuance and dissemination of credentials within different trust domains"
- **Defines the *Security Token Service (STS):***
  - Request security tokens
  - Validate security tokens
  - Exchange security tokens
- **IBM Tivoli Federated Identity Manager (TFIM) implements a STS which provides:**
  - Token mediation (validation, mapping, issuance)
  - Identity mediation
  - Authorization (via TAM)
  - Auditing (to CARS)

SOA Credential Translation – using TFIM

- **Integrate identities for web services / SOA environment**
- **Implement centralized identity mediation & token mapping across multiple, diverse enforcement points**
  - DataPower Gateway
  - WebSphere Application Server (WAS)
  - WebSphere Portal
  - Enterprise Service Bus (ESB)
  - WebSphere Message Broker (WMB)
  - .NET environment
  - Java2 Connector (i.e JDBC)
  - CICS protected by RACF
  - SAP Integration
  - InfoCard for consumer identities
  - ITCAM for SOA for identity-based monitoring
  - Custom token types

Secure Token Service

(Tivoli Federated Identity Manager)

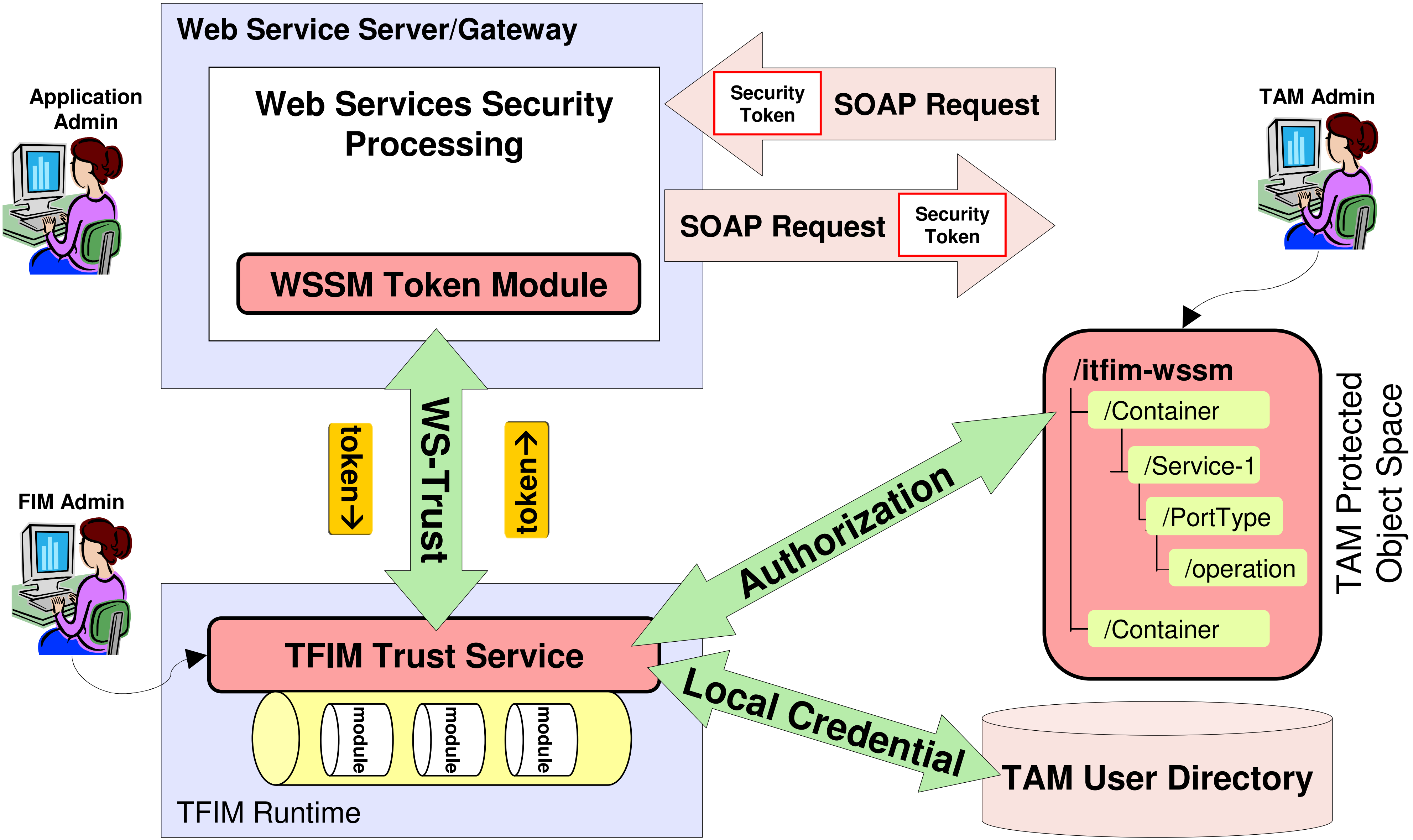


SAML
X.509v3 cert
Kerberos
RACF Passticket
TAM cred
JAAS Principal

SAML
TAM cred
RACF Passticket
JAAS Principal
Kerberos

End-to-End Identity Propagation in a SOA environment

TFIM – Generic Design Overview



Customer Example

- **Client: An Immigration Agency**
- **Country: Asia Pacific**
- **Industry: Government**
- **TFIM Use Case: Identity Service**
- **Current state of deployment, details of timelines (production/pilot/PoC):**
  In production since early 2007

Business Requirement

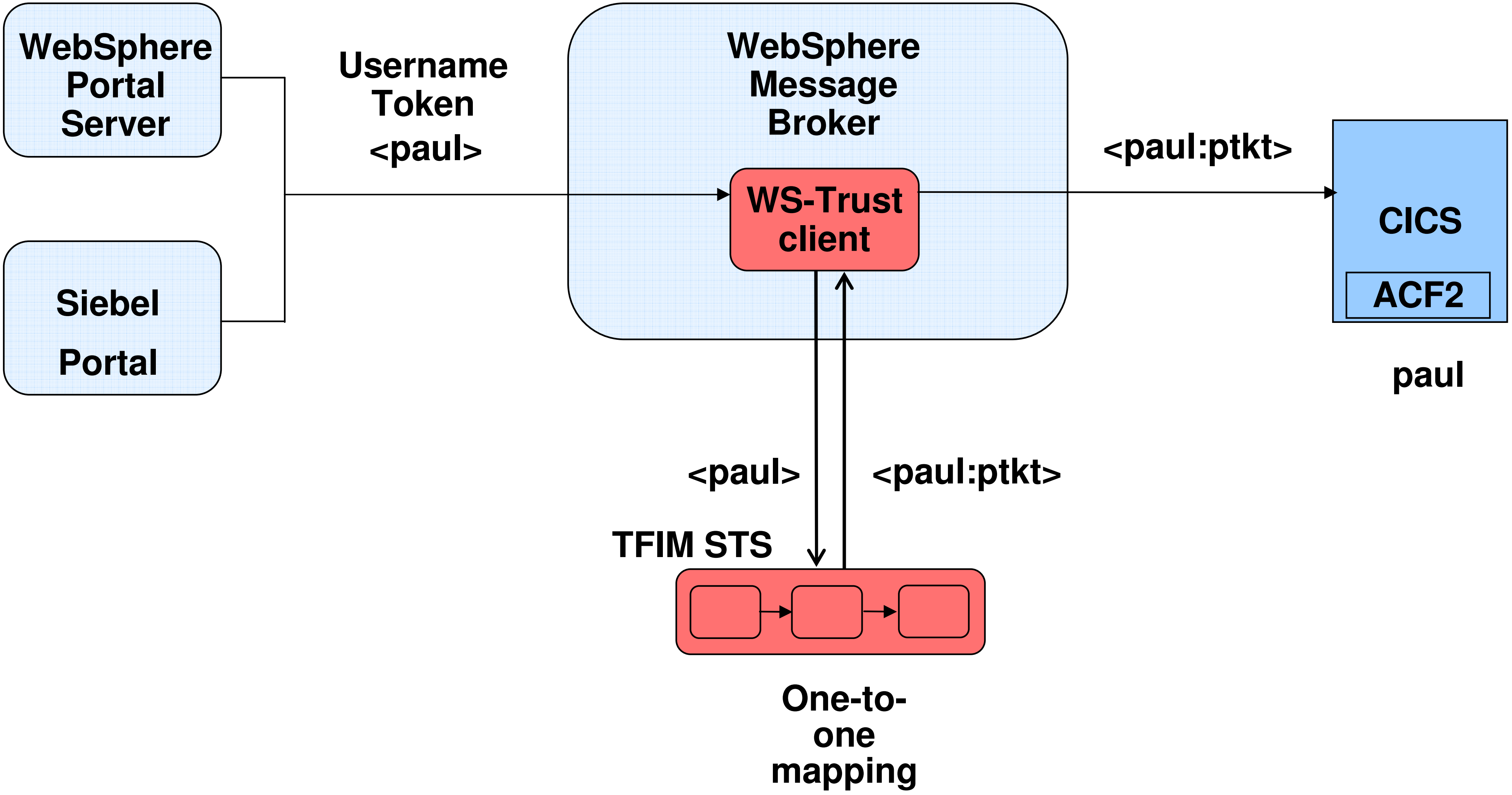
- **The business requirement is to create a new front end for the immigration agency staff.**

- **Instead of accessing a variety of legacy mainframe applications using terminal style interfaces, the staff should have a consolidated view via a Portal interface.**

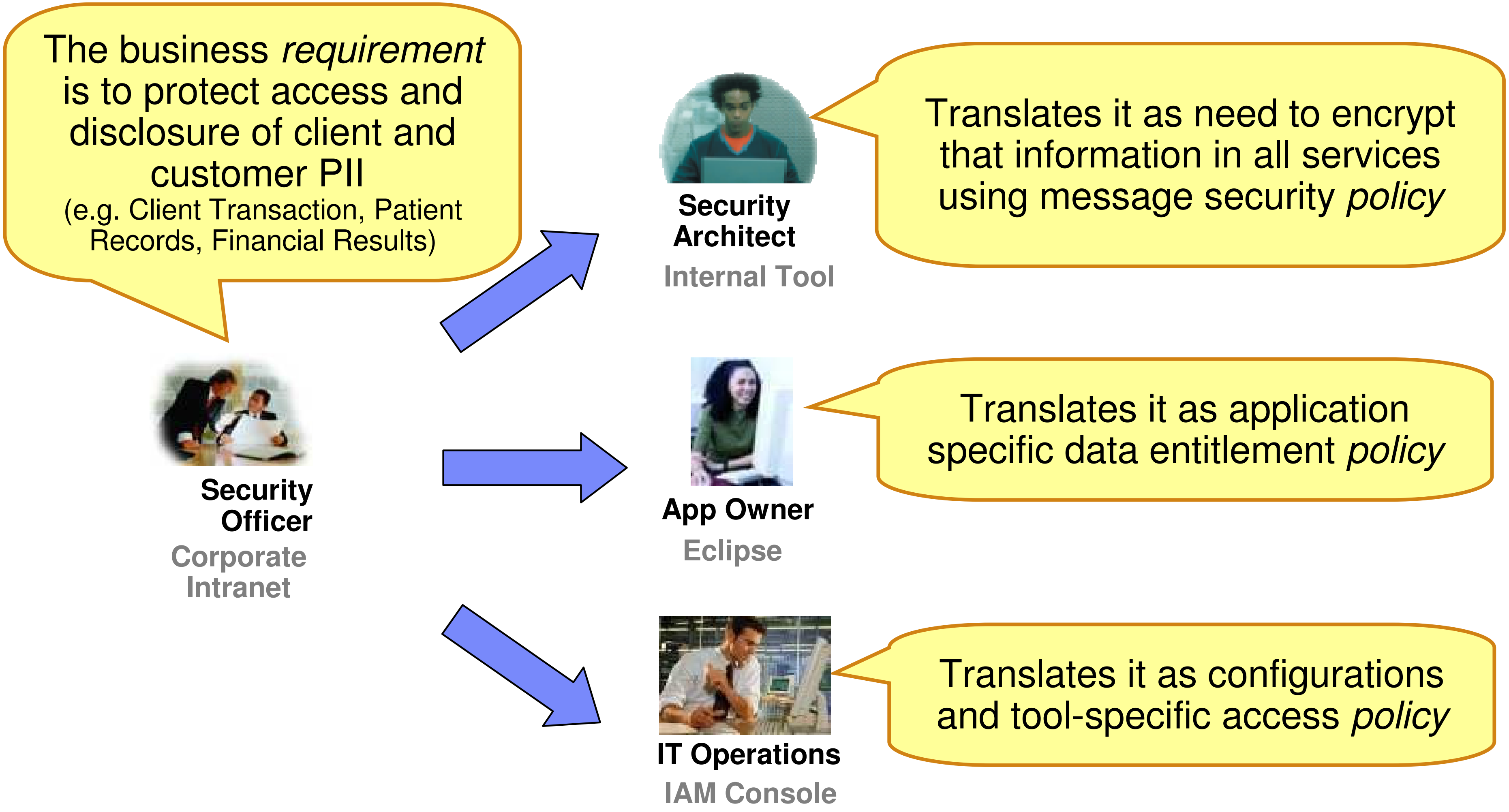
- **In the current deployment the users are all employees (6000+). Later, Internet users (millions) may be added.**

- **The web service “enabling” of the legacy systems requires a new approach for propagating and mapping identities.**

Architecture (brief description + picture)



Today’s Challenge: *How to apply entitlements consistently?*



The business *requirement* is to protect access and disclosure of client and customer PII
(e.g. Client Transaction, Patient Records, Financial Results)

Security Officer
Corporate Intranet

Security Architect
Internal Tool

Translates it as need to encrypt that information in all services using message security *policy*

App Owner
Eclipse

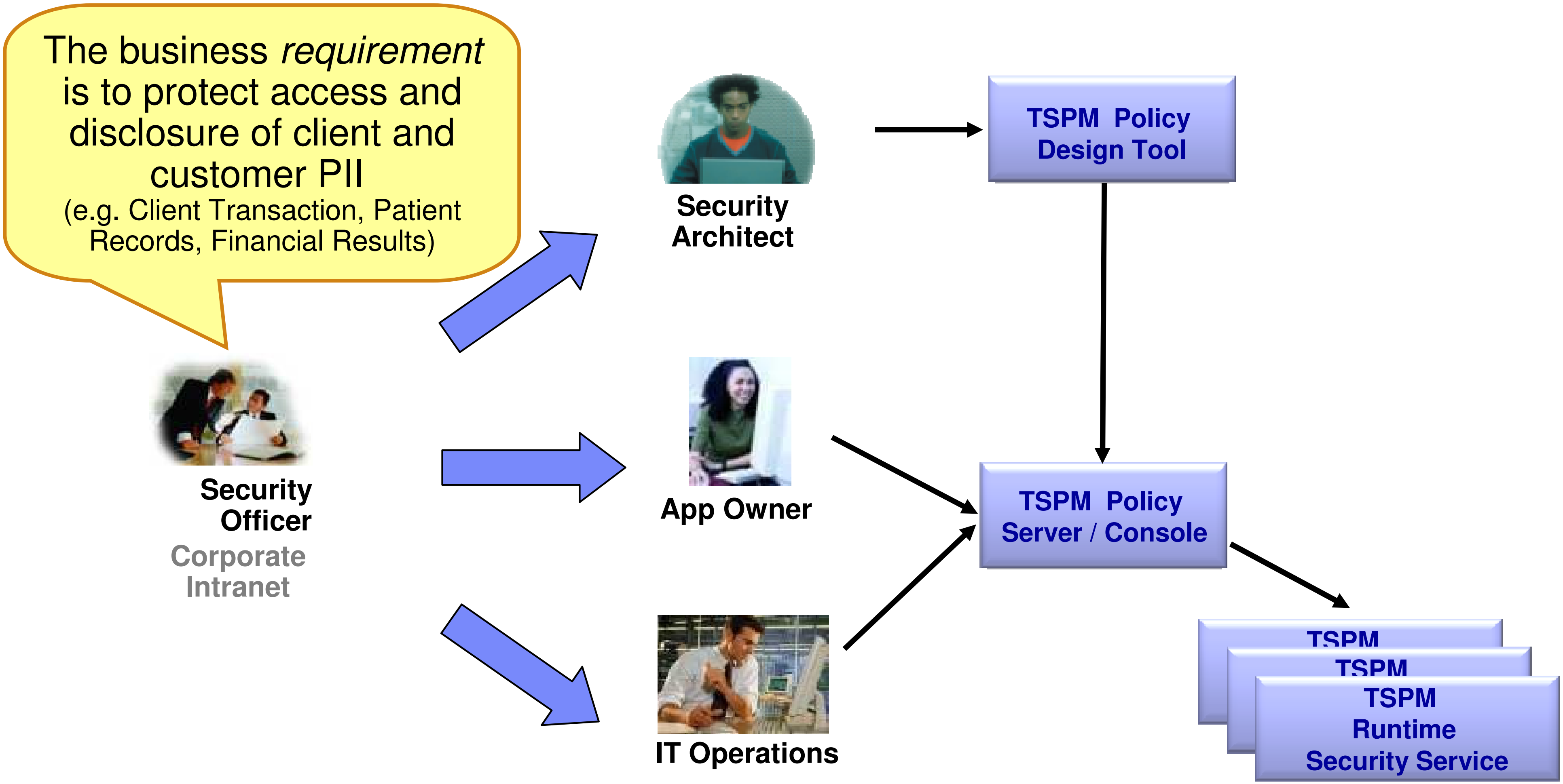
Translates it as application specific data entitlement *policy*

IT Operations
IAM Console

Translates it as configurations and tool-specific access *policy*

How can customers demonstrate compliance back to the business?

IBM Tivoli Security Policy Manager (TSPM) provides the ability consistently define, manage and enforce entitlements across the enterprise



The business *requirement* is to protect access and disclosure of client and customer PII
(e.g. Client Transaction, Patient Records, Financial Results)

Security Officer

Corporate Intranet

Security Architect

App Owner

IT Operations

TSPM Policy Design Tool

TSPM Policy Server / Console

TSPM Runtime Security Service

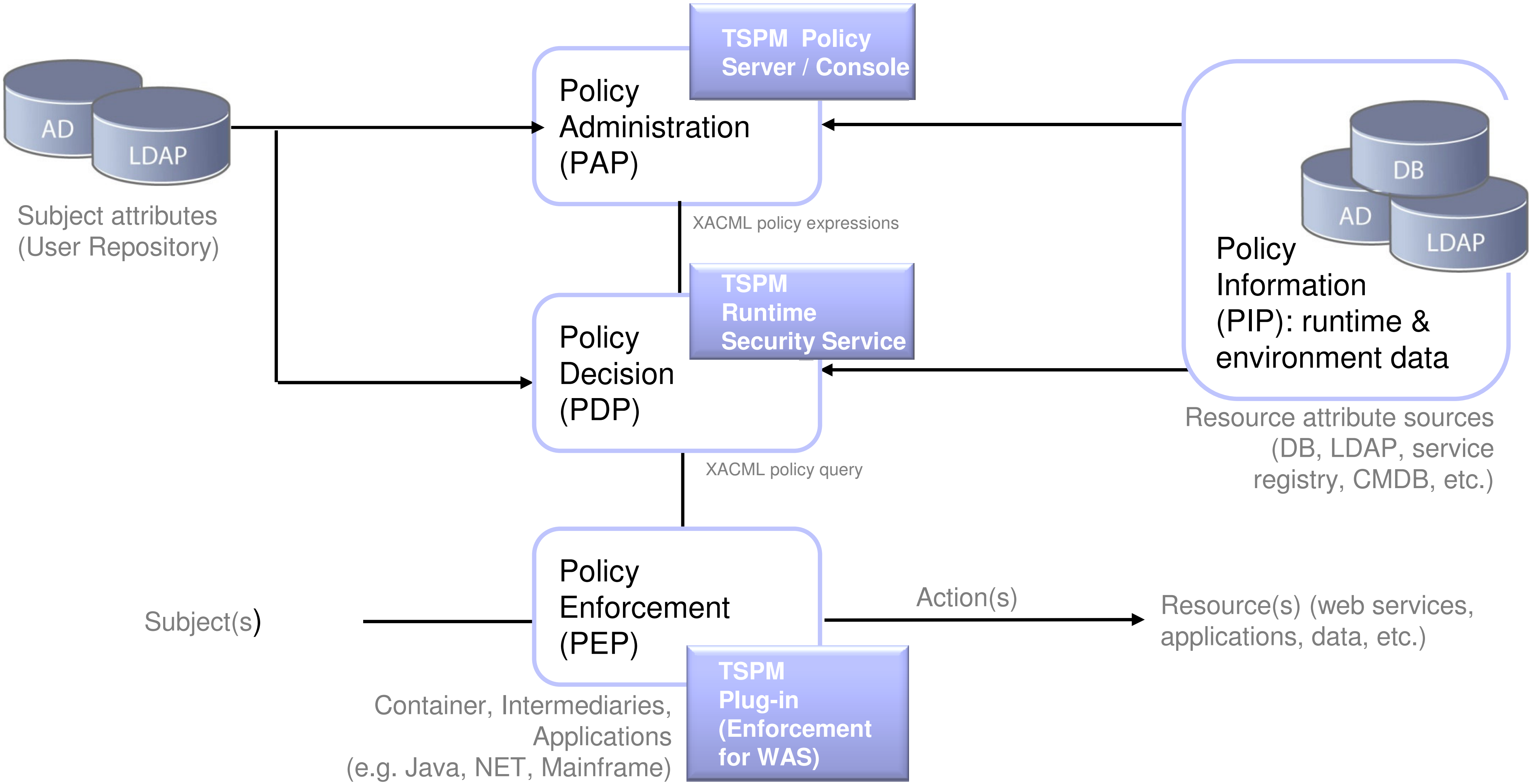
Demonstrate Compliance and Enable Identity Governance

Sample Policy: Who can Access to Approve a Funds transfer?

TSPM provides ability to author entitlement based on one or more conditions

- **Role**
  - The user must be in the `tfr_approver` role
- **Service attribute**
  - The transfer amount must be less than the maximum transfer limit for the type of transfer
- **User attribute**
  - The transfer amount must be less than the maximum transfer limit for the user
- **Relationship**
  - The user must have been assigned responsibility for the source account.
- **Environment**
  - The transfer must be made during business hours and from the corporate network
- **Request/Session Context**
  - The user must have authenticated using 2-factor authentication
- **Other Decision Engines**
  - The transaction must pass the criteria checked by the Fraud Detection system

TSPM Enables Application Owners to Easily Implement Entitlements for New Applications



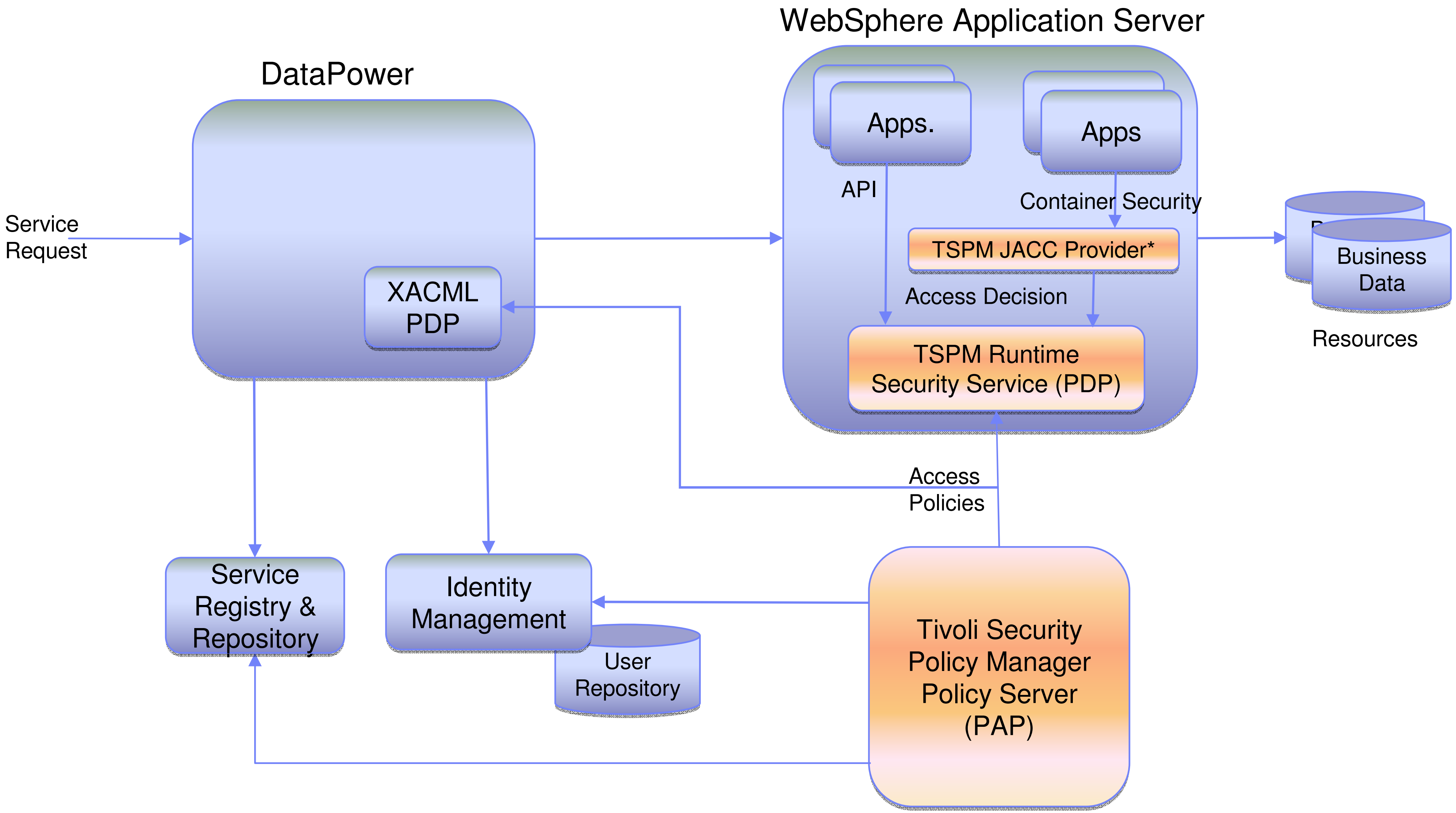
TSPM Policy Server / Console
Policy Administration (PAP)
AD
LDAP
Subject attributes (User Repository)
XACML policy expressions
TSPM Runtime Security Service
Policy Decision (PDP)
DB
AD
LDAP
Policy Information (PIP): runtime & environment data
Resource attribute sources (DB, LDAP, service registry, CMDB, etc.)
XACML policy query
Policy Enforcement (PEP)
Subject(s)
Action(s)
Resource(s) (web services, applications, data, etc.)
Container, Intermediaries, Applications (e.g. Java, NET, Mainframe)
TSPM Plug-in (Enforcement for WAS)

Customer Example

- **Background**
  - Government agency
  - New call center application deployment
  - Primarily Java environment including WAS
  - Existing IAM solution with Tivoli Identity and Access Manager
  - DataPower for XML firewall and web services security

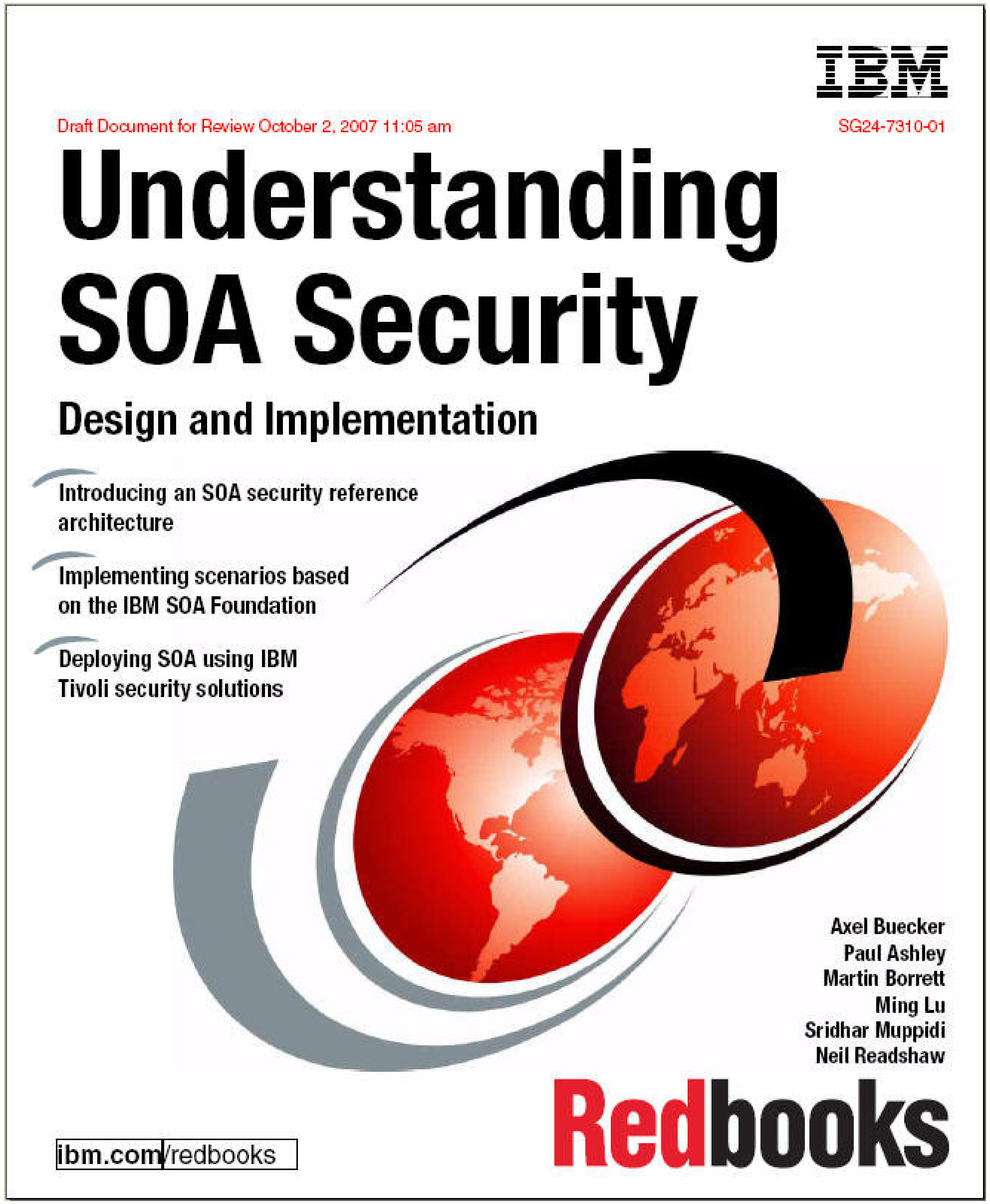
- **Challenges**
  - Need to address compliance concerns and privacy data security
  - How can we provide fine-grained access control including data-level access to employees, contractors and 3rd party partners?

Solution Approach – Government Agency Entitlements



* Currently in beta

http://www.redbooks.ibm.com/redpieces/abstracts/sg247310.html?Open



IBM

Draft Document for Review October 2, 2007 11:05 am

SG24-7310-01

Understanding SOA Security

Design and Implementation

Introducing an SOA security reference architecture

Implementing scenarios based on the IBM SOA Foundation

Deploying SOA using IBM Tivoli security solutions

Axel Buecker
Paul Ashley
Martin Borrett
Ming Lu
Sridhar Muppidi
Neil Readshaw

Redbooks

ibm.com/redbooks

Summary

- **Issues well understood**
- **Standards and adoption of standards continues to mature**
- **Technology exists today to address security issues**
- **Customers are making progress in meeting business/security requirements**
- **IBM can help**