



# Seguridad en ambientes SOA

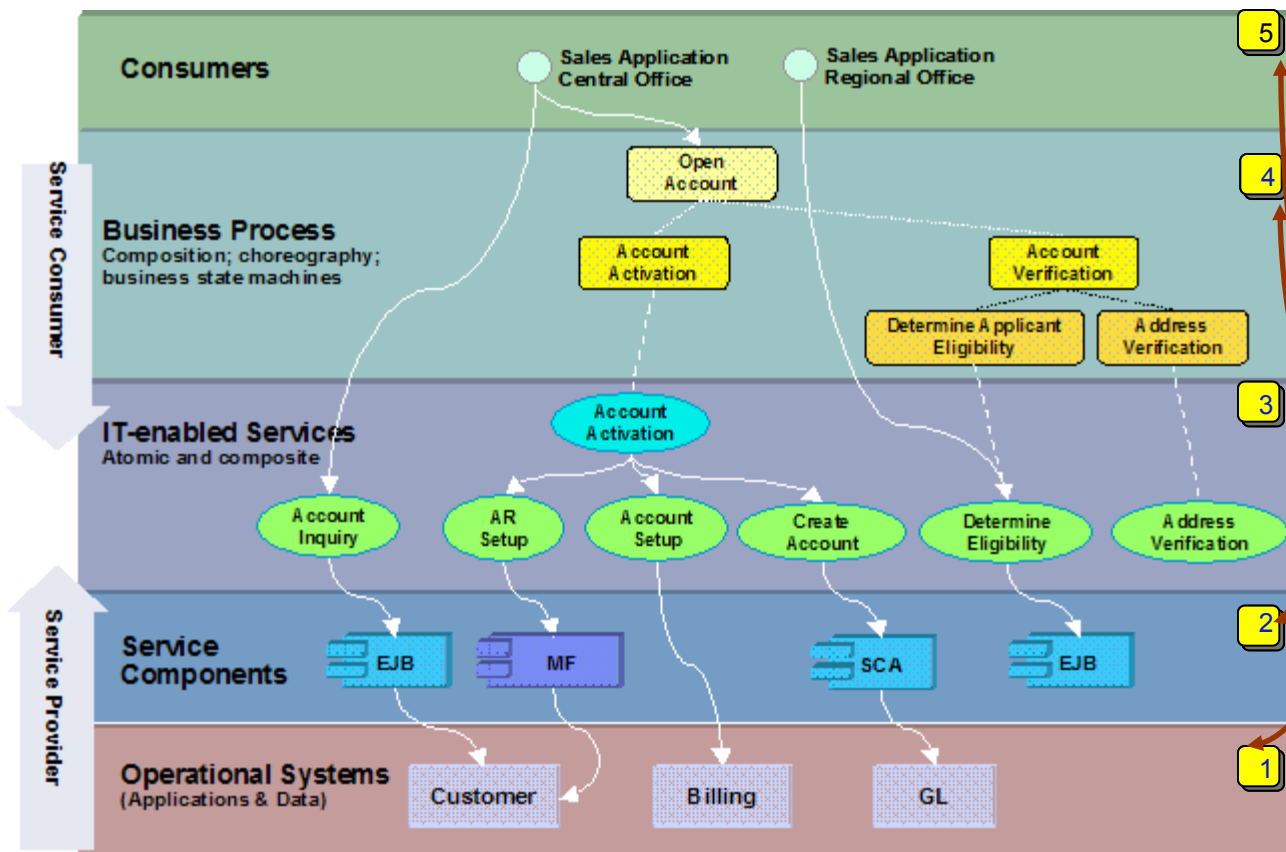
Retos, patrones y soluciones

Eduardo Solis  
Eric Wood  
Sridhar Muppidi  
IBM Software Group

# Agenda

- Consideraciones de seguridad en SOA
- Soluciones de IBM
  - Modelo referencia de seguridad en SOA
- Ejemplos de soluciones de IBM
  - Protección de mensajes
  - Mediación de identidades
  - Administración de políticas de seguridad
- Comentarios finales y preguntas

# La seguridad en SOA abarca todas las capas de la solución



## Seguridad SOA

- Identidad
- Autenticación
- Autorización y privacidad.
- Auditoria
- Confidencialidad, integridad y disponibilidad
- Compliance
- Administración y manejo de políticas.

# Consideraciones de Seguridad en SOA

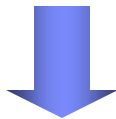
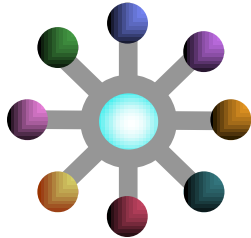
- Entidades/Identidades – usuarios, servicios
  - Los servicios tienen identidades
  - Identidades y/o credenciales se propagan a través de los servicios
- Usuarios y servicios son sujetos a los mismos mecanismos de control de seguridad.
- Limites organizacionales/empresariales
  - Perímetros no son claros
  - Las identidades son administradas más allá de los límites
- Relaciones de confianza son establecidas más allá de los limites
  - Composición de aplicaciones
  - Necesidad de garantizar controles de seguridad correctos para cada servicio y para la combinación de estos.
- Mayor enfoque en datos/información
  - Protección de datos en tránsito y estáticos
  - Medidas de protección consistentes
  - Garantías de disponibilidad de datos
- Gobernabilidad, Riesgo y Compliance
  - Auditoria, identificación de transacciones,

# SOA Criterio de entrada – Orientado al negocio y enfocado a TI

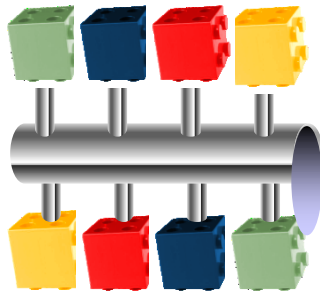
		Qué es?	Valor
Peop		Proporcionar interacciones basadas en roles y colaboración a través de servicios	Mejorar productividad y flexibilidad habilitando interacciones de usuarios orientadas a procesos de negocio.
Proces		Lograr innovación de procesos de negocio tratando cada tarea como un servicio modular.	Mayor innovación y flexibilidad a través de implementaciones rápidas y modificación de procesos de negocio
Information		Proveer información confiable en contexto del negocio tratándolo como un servicio.	Mejores operaciones de negocio, decisiones mejor informadas y reducción de riesgos con información entregada en línea y en contexto
Reuse		Habilitar infraestructura existente como un servicio y completar la infraestructura con nuevos servicios	Disminución de riesgos y tiempo de desarrollo aprovechando funcionalidad comprobada y probada con tiempo.
Connectivity		Conectar sistemas, usuarios y canales de negocios basados en estándares abiertos	Reducción de costos de mantenimiento y mayor confiabilidad y consistencia usando relaciones flexibles y multi-punto

# Retos de seguridad en ambientes SOA existentes

Integración de aplicaciones empresariales (EAI)



Integración orientada a servicios



## ■ Identidad

- Cambios de identidad o de acceso requieren cambios en la aplicación.
- Imposible re-utilizar servicios si la lógica de seguridad está en el código

## ■ Protección

- Incremento de la importancia del contexto tanto a nivel de mensajes como de aplicación
- Necesidad de externalizar la lógica de seguridad para proteger accesos consistentemente

## ■ Compliance

- Quién hace los cambios de identidad y control de acceso? Desarrolladores?
- Como se auditan y garantizan los controles de negocio? Cual es el riesgo de una violación?

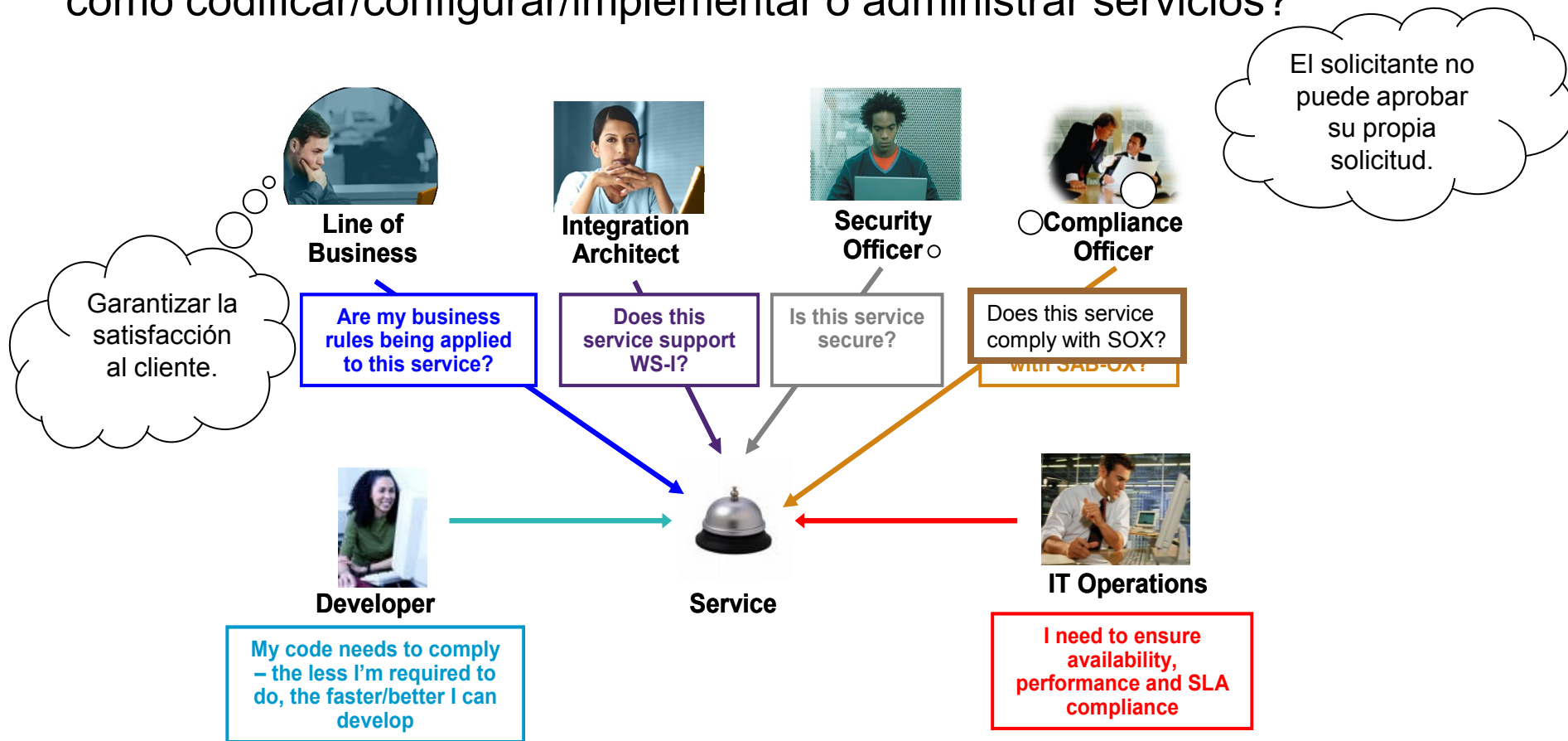


# Soluciones



# Actores en una empresa y sus expectativas

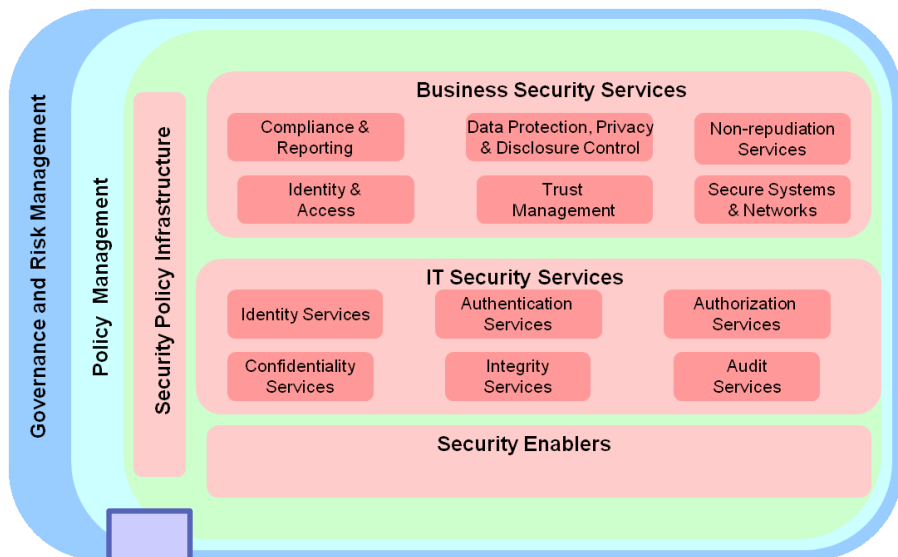
- Múltiples roles interactúan de distintas maneras con los servicios
- Como satisfacer las necesidades sin requerir que los actores sepan como codificar/configurar/implementar o administrar servicios?



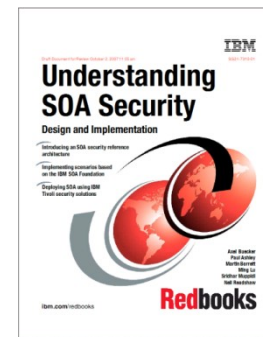
# Principios arquitectónicos

- Ejecución consistente de políticas (Tiempo de Ejecución)
  - Seguridad como un servicio – Orientación a servicio
  - Federación mediante mediación
  
- Separar políticas de aplicación
  - Flexibilidad al lidiar con cambios
  - No necesariamente significa tener que reescribir las aplicaciones
  
- Administración consistente de políticas (Administración)
  - Federación de políticas
  
- Experiencia
  - Modelos de seguridad
  
- Interoperabilidad e integración
  - Enfoque abierto estándares abiertos y open source

# Security and Policy reference models



Seguridad



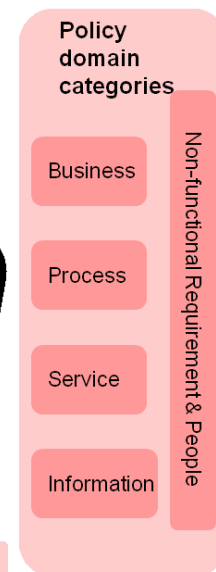
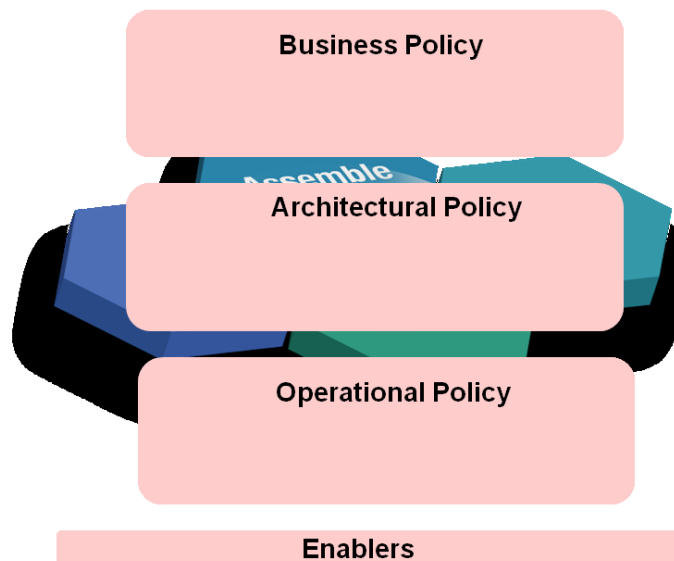
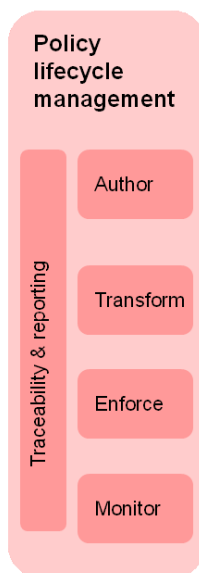
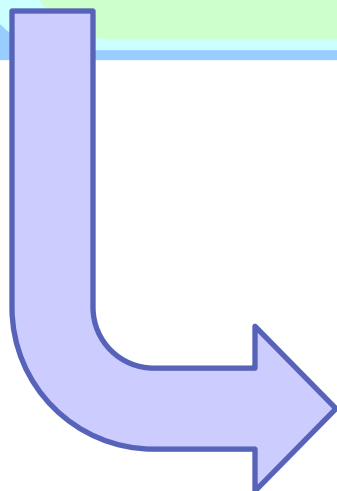
SG24-7310-01

Política

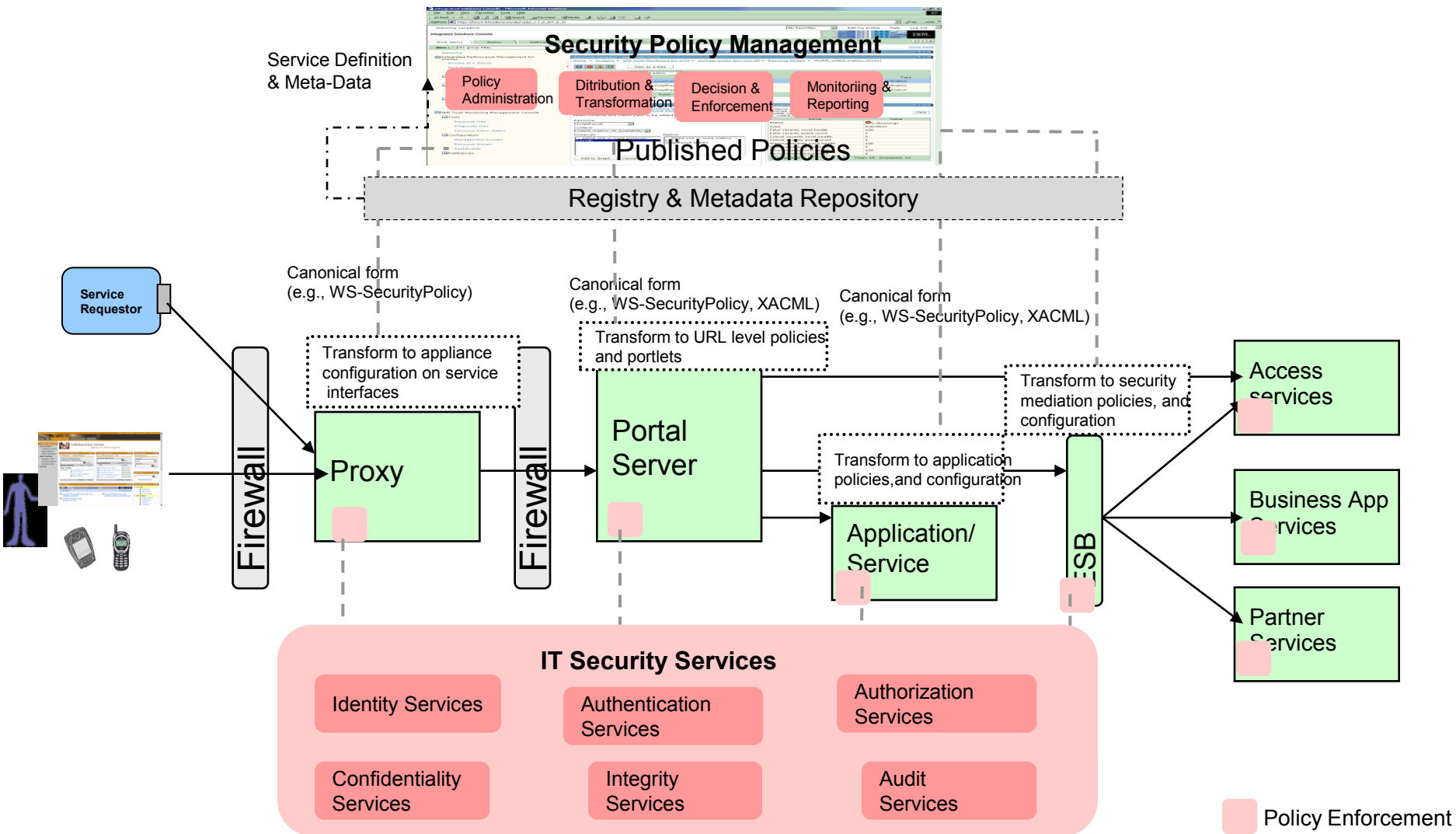
Lifecycle stages

Abstraction Levels

Policy domains

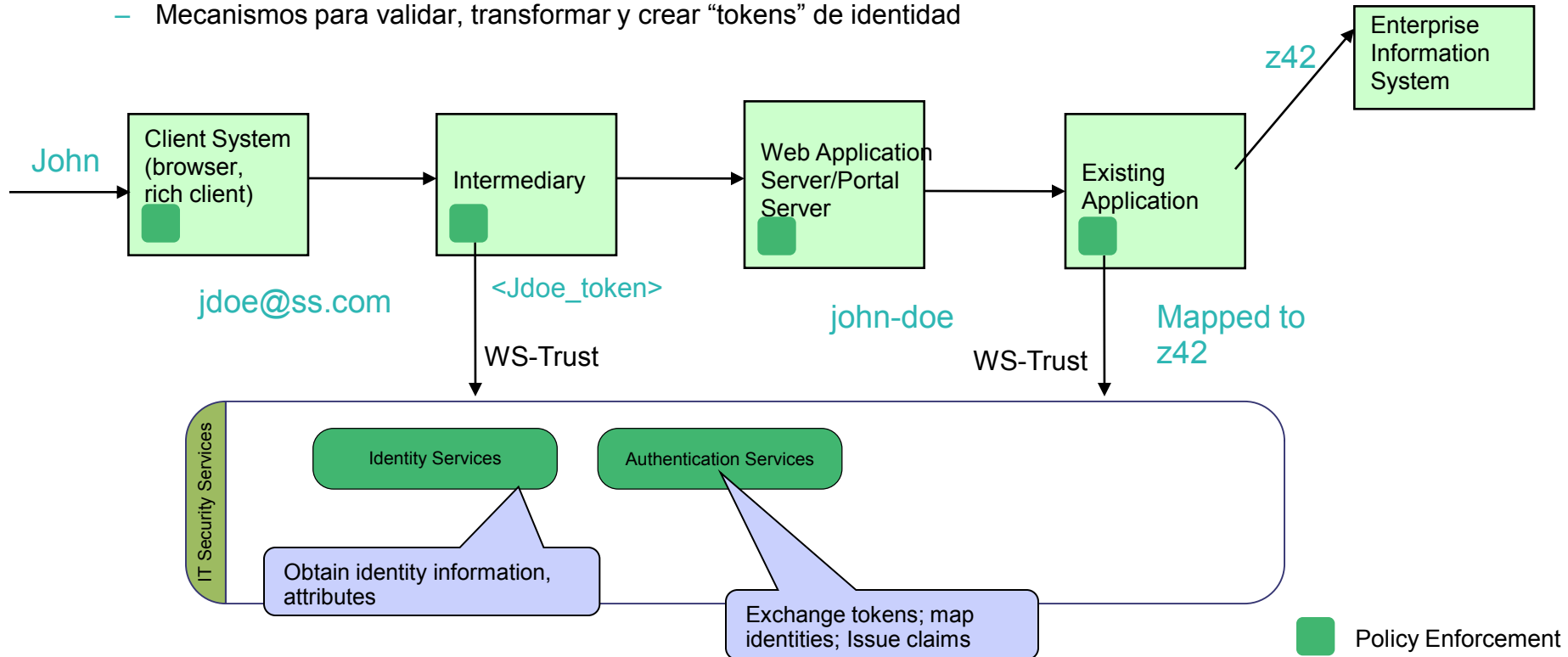


# Administración consistente de políticas y aplicación efectiva en tiempo de ejecución



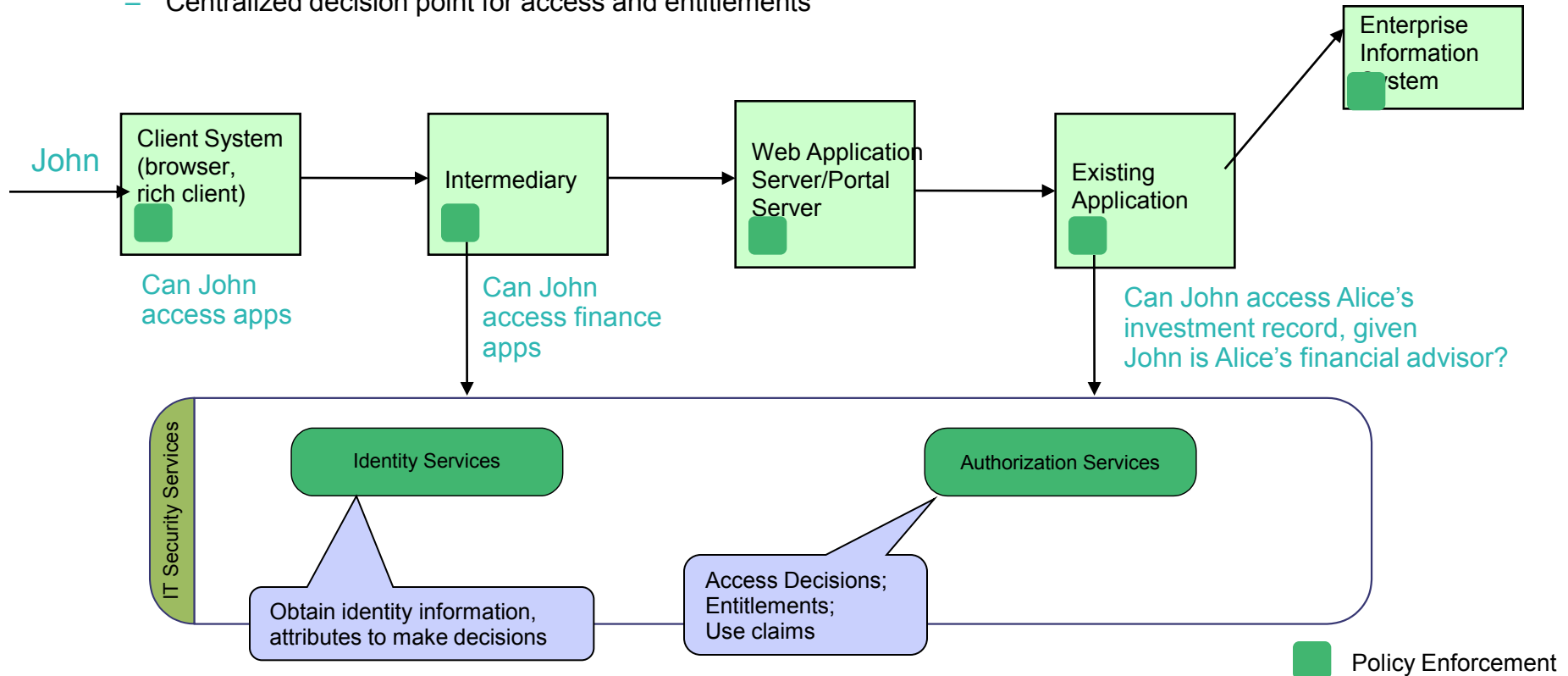
# Ejemplo: Autenticación y propagación de identidad

- Las aplicaciones necesitan saber la identidad del usuario para controlar acceso y garantizar compliance
  - Acomplamiento flojo y multiples dominios de seguridad introducen retos
- Información sobre identidad debe ser mediada
- Servicio de Identidad (WS-Trust)
  - Mecanismos para validar, transformar y crear "tokens" de identidad

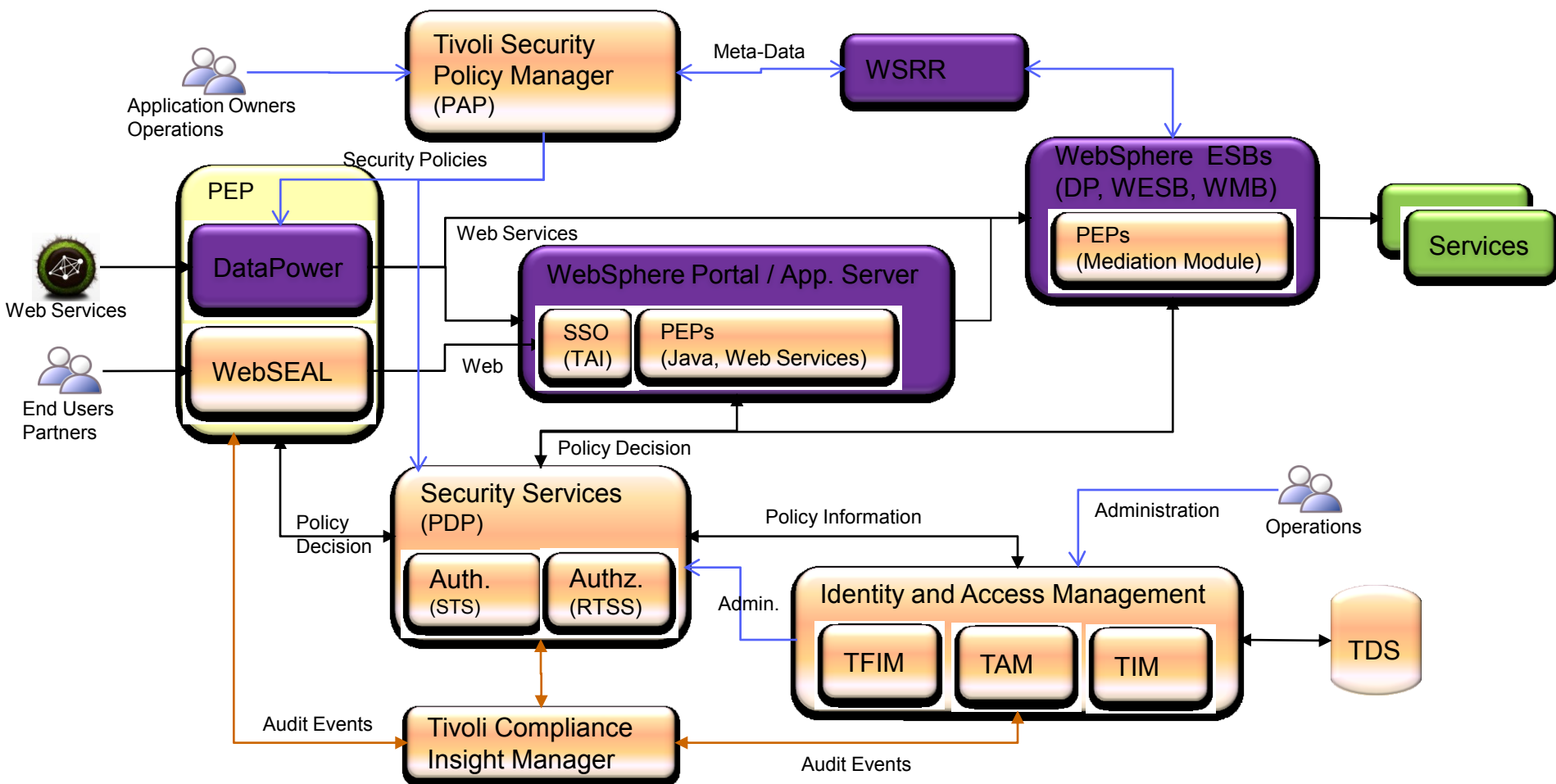


# Example: Authorization

- Access decisions to take following into considerations
  - Identity context, resource context, environment context, business context
- Need an efficient way to externalize access control out of application logic
- Authorization service (XACML)
  - Centralized decision point for access and entitlements



# Ejemplo de Integración: WebSphere y soluciones de seguridad Tivoli



WSRR: WebSphere Service Registry and Repository; DP: WebSphere DataPower; WESB: WebSphere Enterprise Service Bus; WMB: WebSphere Message Broker; TFIM: Tivoli Federated Identity Manager; TAM: Tivoli Access Manager; TIM: Tivoli Identity Manager; TDS: Tivoli Directory Server; TSPM: Tivoli Security Policy Manager; RTSS: Runtime Security Service; STS: Secure Token Service; PAP: Policy Administration Point; PDP: Policy Decision Point; PEP: Policy Enforcement Point



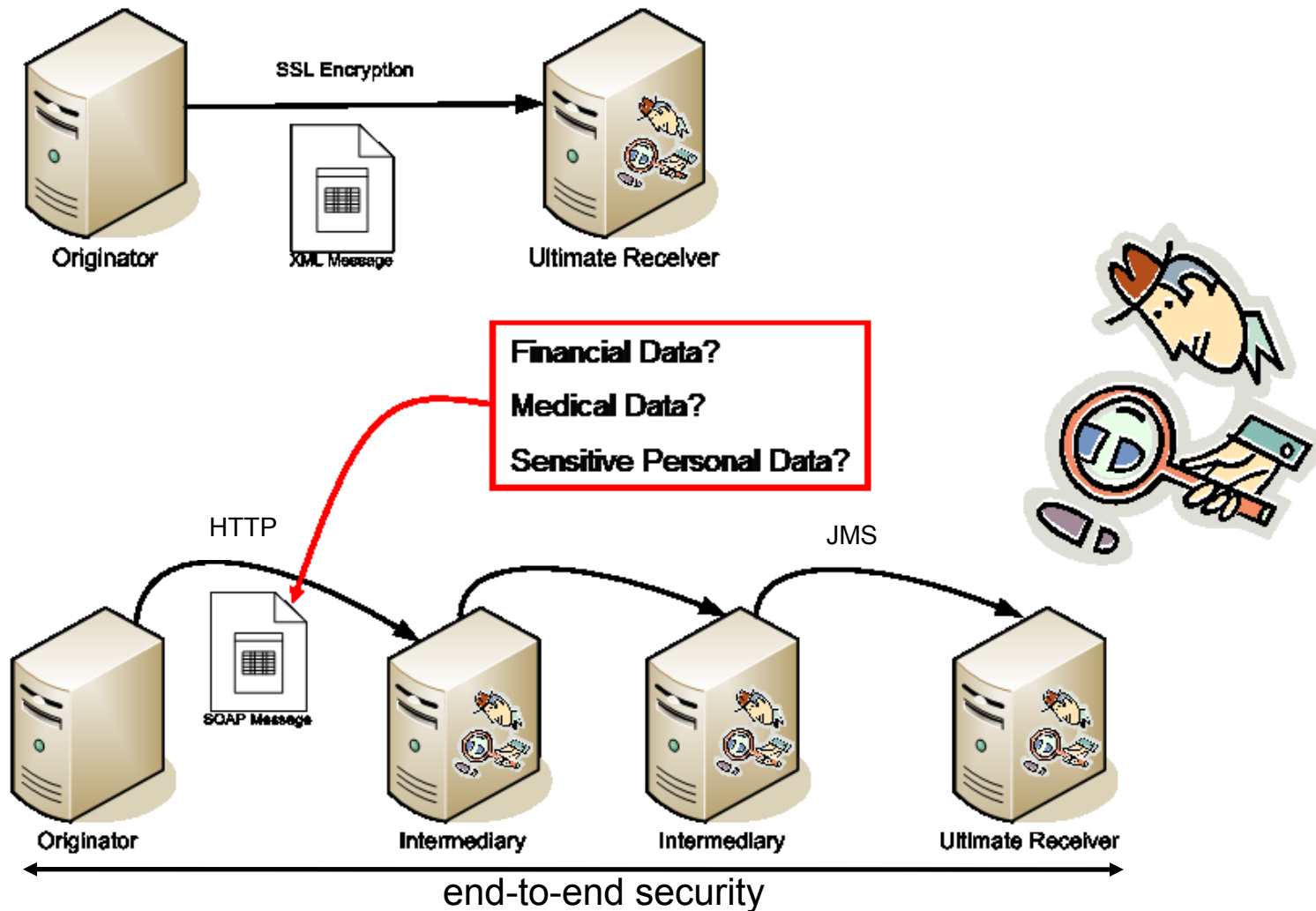
# Ejemplo de soluciones IBM



# Patrones de soluciones emergentes originadas por clientes y puntos de entrada SOA

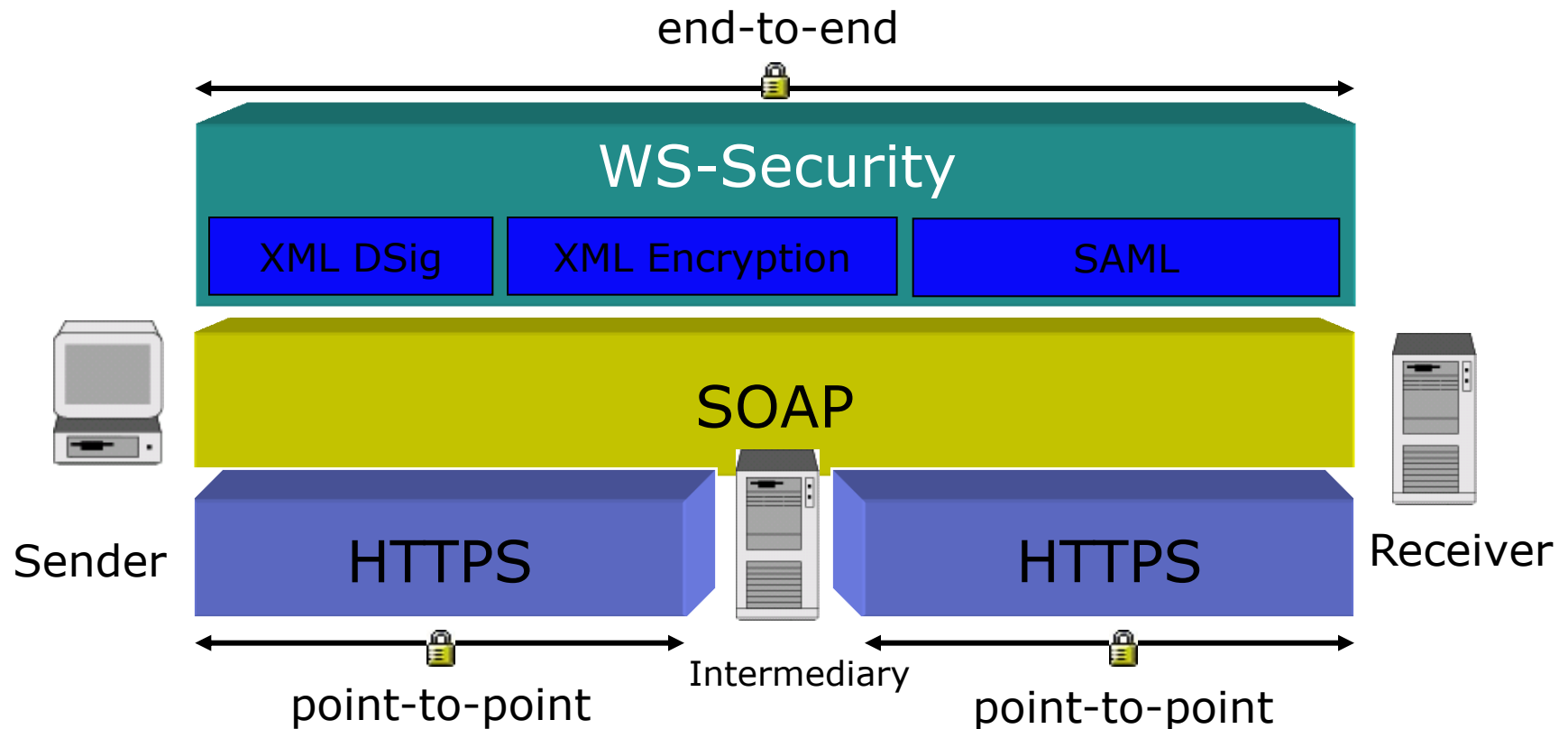
- Protección de mensajes
  - Proteger acceso a servicios web
  
- Mediación de identidad
  - Entre servicios web en mutiples dominios
  - Acceso a sistemas existentes (Legacy)
  - Implemetaciones ESB federadas
  - Agregar identidad a servicios externos
  
- Administración de políticas de seguridad y Compliance
  - Administración unificada de políticas
  - Servicios de seguridad en tiempo de ejecución
    - Atributos de identidad, autenticación y servicios de identidad
    - Autorización y servicio de administración de derechos

# Protección de mensajes requiere nuevas capas de seguridad



# Soluciones para seguridad en mensajes basadas en estándares

- WS-Security define firma y cifrado de “mensajes”
  - Provee seguridad punto-a-punto con consideraciones multi-dominio
  - “Caro” así que usar moderadamente – SSL es suficiente dentro de un dominio
  - Implementado e middleware



# Transport Security v/s Message Security

## ▪ Benefits of Transport Level (SSL/TLS)

- HTTPS transport can be used to provide a very fast and secure transport of Web services
- Provides authentication through either HTTP Basic or Client certificates (X.509)
- Provides integrity between client and HTTP server by using asymmetric key cryptography to establish authenticity of server and client and to securely share a secret key
- Provides confidentiality between client and HTTP server through efficient shared key cryptography
- Has good support for a broad array of hardware accelerators
- Is mature and similarly implemented by most vendors and thus, subject to few interoperability problems

## ▪ When to use transport level security

- High transaction volume (Fast and scales well)
- No intermediary processing (filtering or some form of content-based routing)
- Interoperability issues associated with the emerging WSS implementations
  - SSL is mature and SSL implementations from different vendors interoperate well
- Secure attachments to Web services
  - SSL encrypts all of the transport level packets, the Web service headers, body and attachments are all secured (i.e. **transient security**)

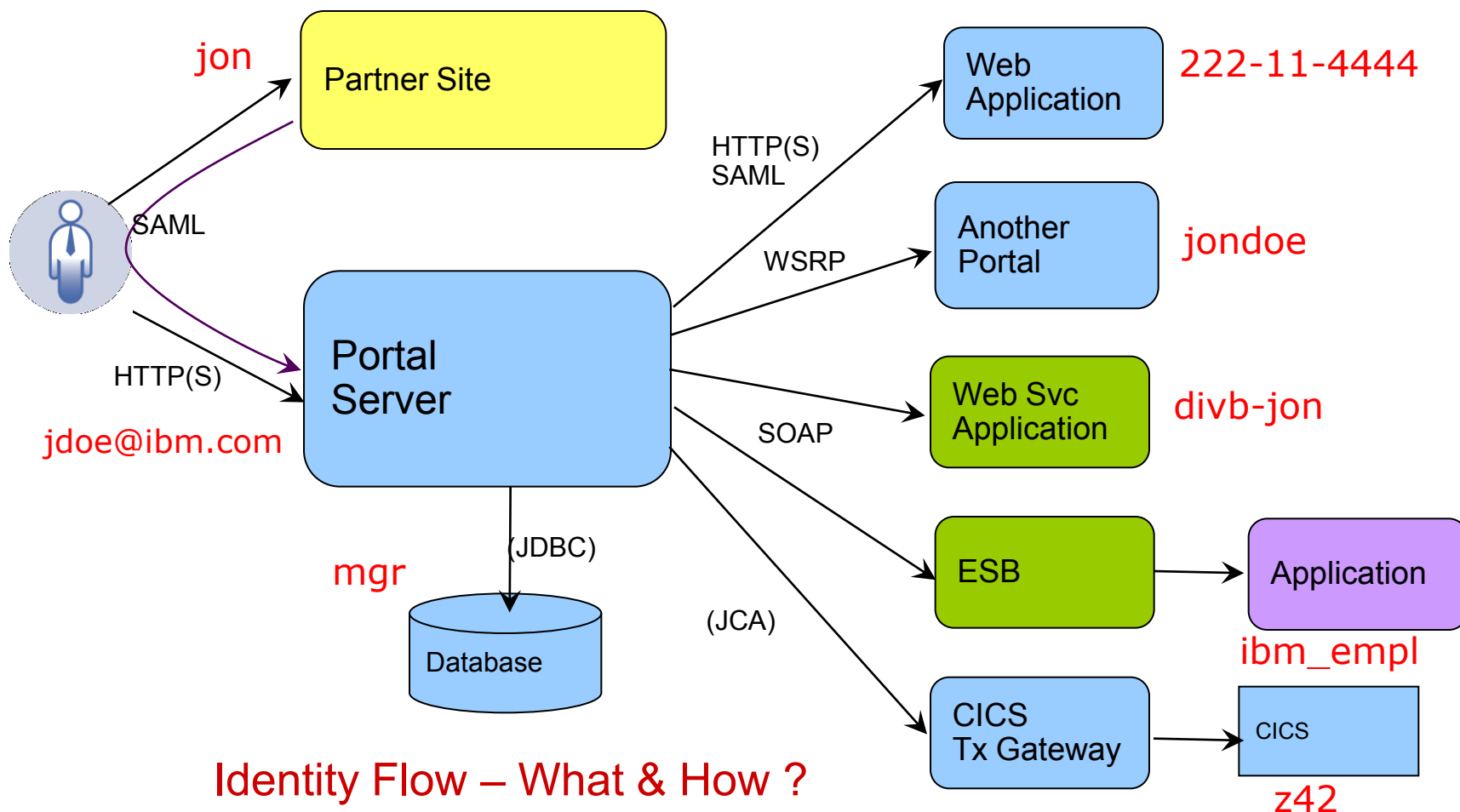
## ▪ Benefits of using Message Level (WS-Security)

- End-to-end security through any number of intermediaries (i.e. **persistent security**)
- Integrity and confidentiality of selective elements in message header and/or body
  - Parts of message can be encrypted for a particular SOAP node
  - XML Signatures can be applied across the whole SOAP Body, and/or the userNameToken, and/or generated TimeStamp to provide integrity or prove the possession of the private key
- Profiles for interoperable security tokens, Extensibility for custom security tokens & Propagation of security context
- Foundation for Web Services Security roadmap
  - WS-Policy, WS-Trust, WS-SecurityPolicy, WS-Federation, WS-SecureConversation

## ▪ When to use message level security

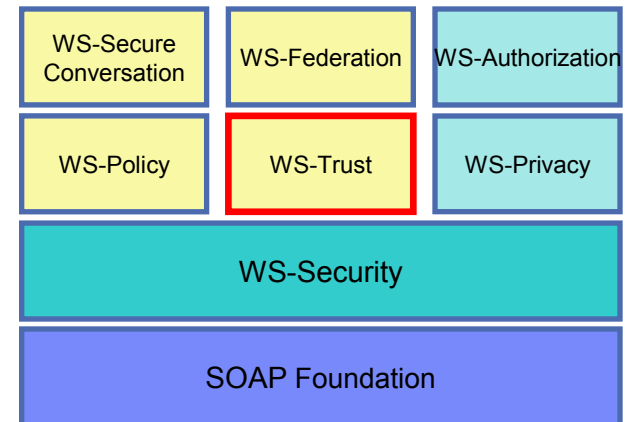
- Intermediaries encrypt some parts of the message while leaving other parts in the clear
- Message origin authentication (what/who sent the message)
- Persistent security for messages
  - The message integrity and confidentiality persist beyond a transport connection
- Future development
  - To enable federation, secure sessions, and policy based security for Web services utilizing Web Services Roadmap

# Propagación de identidad es importante



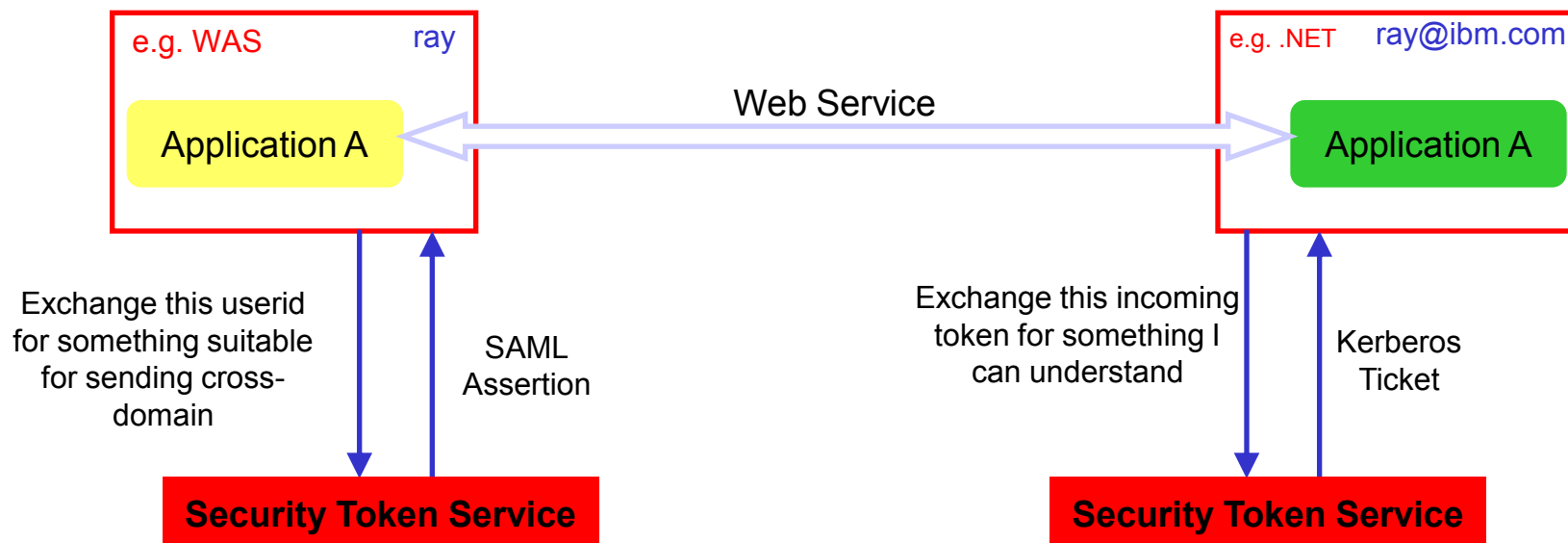
# Soluciones basadas en estándares

- Servicio estándar para solucionar problemas con el flujo de identidad
  - Qué identidad es entregada y
  - Cómo es entregada.
- WS-Trust define mecanismos para:
  - “...intercambio de tokens de seguridad para habilitar expedición y diseminación de credenciales en distintos dominios de confianza”
- Define el *Security Token Service (STS)*:
  - Pedir un token de seguridad
  - Validar tokens de seguridad
  - Intercambiar tokens de seguridad



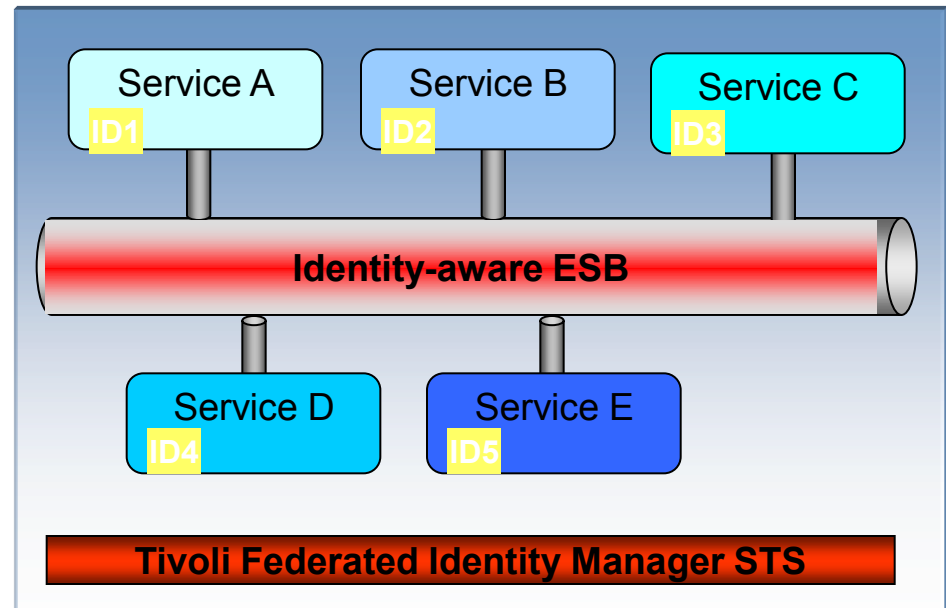
# Patrón: Implementación de servicio web multi-dominio

- Capacidad de interoperación entre servidores aplicativos
  - Aserciones SAML orientadas para transportar identidad a través de dominios



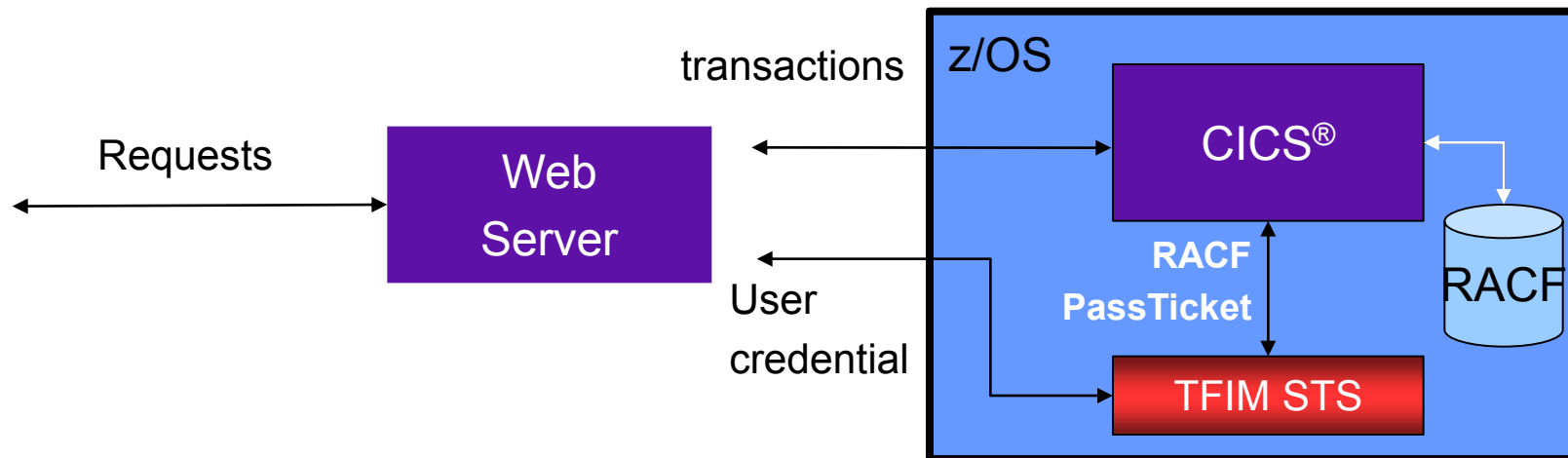
# SOA requires abstracción de identidad para lograr procesar identidad fuera de la aplicación

- Los servicios tienen identidades (al igual que los usuarios)
- STS de IBM
  - Tivoli Federated Identity Manager
- Hacer que el ESB sea “identity-aware”
  - WebSphere Enterprise Service Bus
  - WebSphere Message Broker
  - WebSphere DataPower
- Reduce costo de código redundante en las aplicaciones.



# Propagar Identidades auditables a Mainframe usando RACF PassTicket

- Flujo auditable de identidad entre mainframe y aplicaciones distribuidas para cumplir con requerimientos “trazables: (auditorias, compliance)
  - ▶ Entrega procesos de autenticación conectables
  - ▶ Preserva la granularidad de la identidad del usuario
  - ▶ Utiliza mecanismos de auditoria de z/OS para mejorar compliance

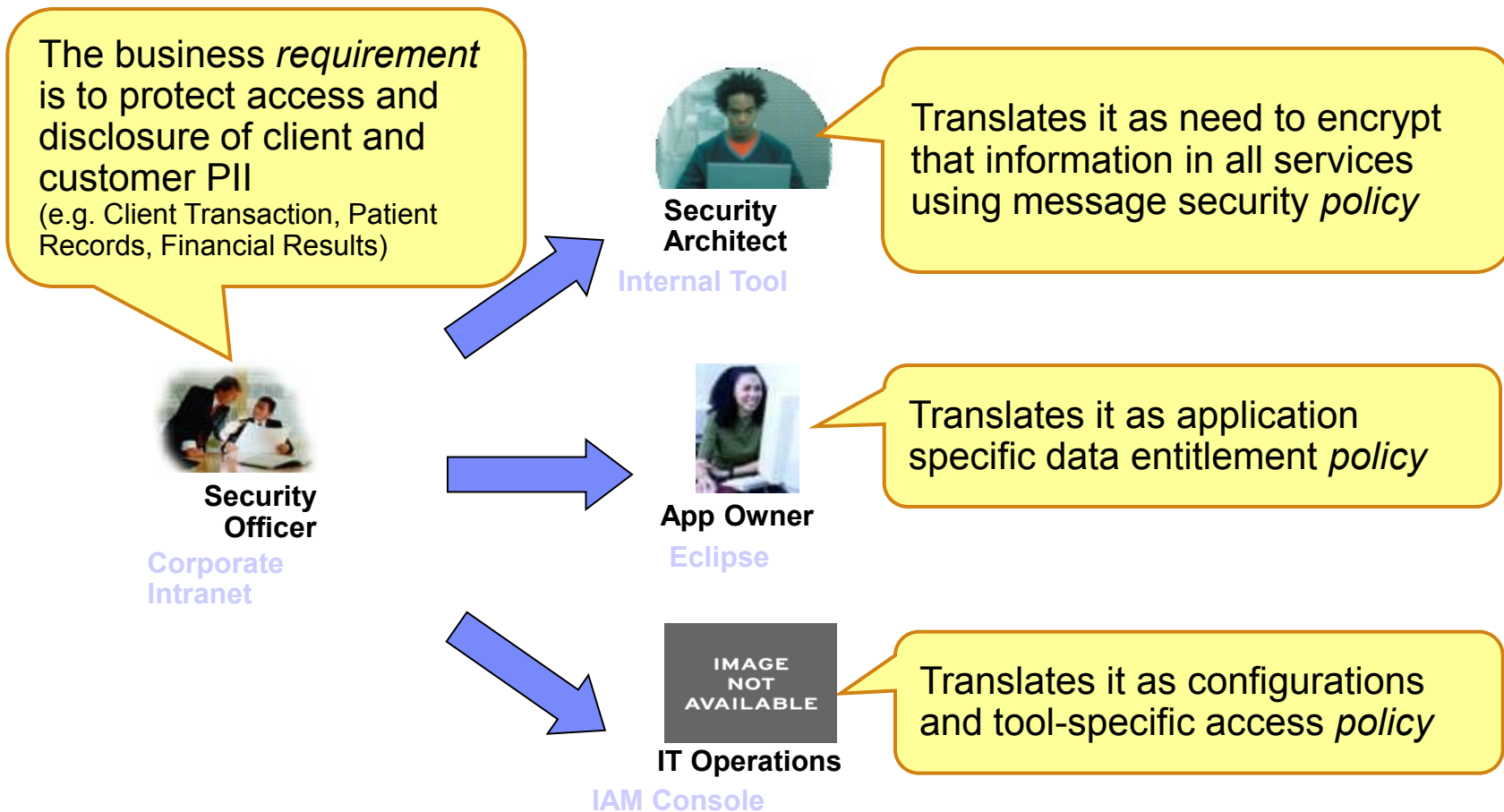


## What are the New & Emerging Challenges for Application Security?

- **Business Transaction and Application Compliance**
  - Increasing regulations requires **deeper** access control
  - Need roles-, rules- and attributes-based access control
- **Data and Information Sharing**
  - Increasing cost of application security development
  - Increasing risk of Intellectual Property Theft (e.g. \$60K per app)
  - Need centralized entitlement and data-level access control
- **Increasing Collaboration and SOA**
  - Rapid deployment of web services and access risk
  - Need consistent security policy & context-based access control
- **Increasing Numbers and Greater Diversity of Users**
  - Increasing diversity and growth in user base
  - Need personalization, catalog and portal/portlet level entitlements for secure access control
- **Heterogeneity → Costly Security Administration**
  - Requires standards-based interoperability and support (WS-Trust, XACML)
  - Need common, pluggable framework for authentication, authorization and audit

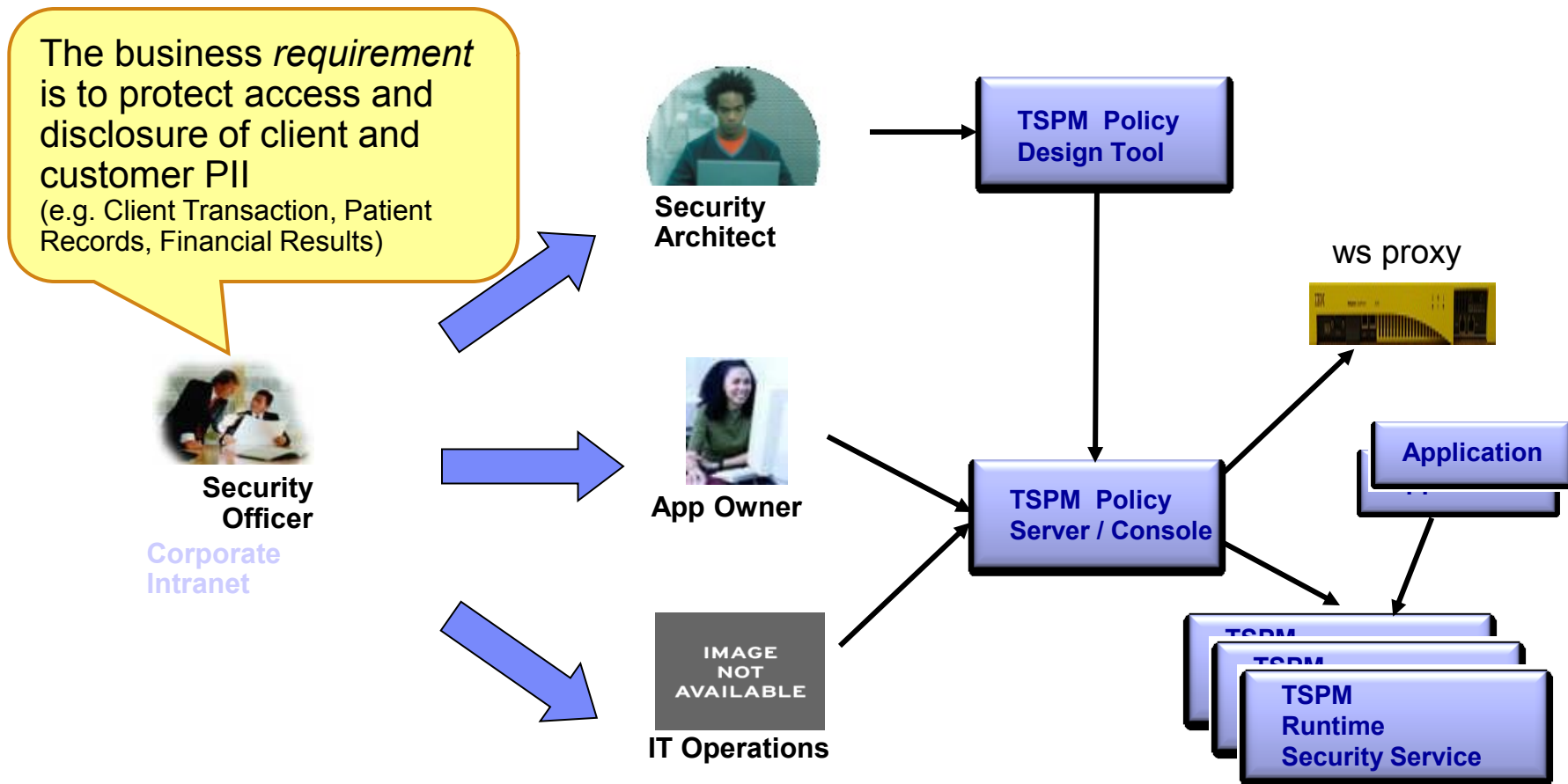


# Today's Challenge: How to apply entitlements consistently?



How can customers demonstrate compliance back to the business?

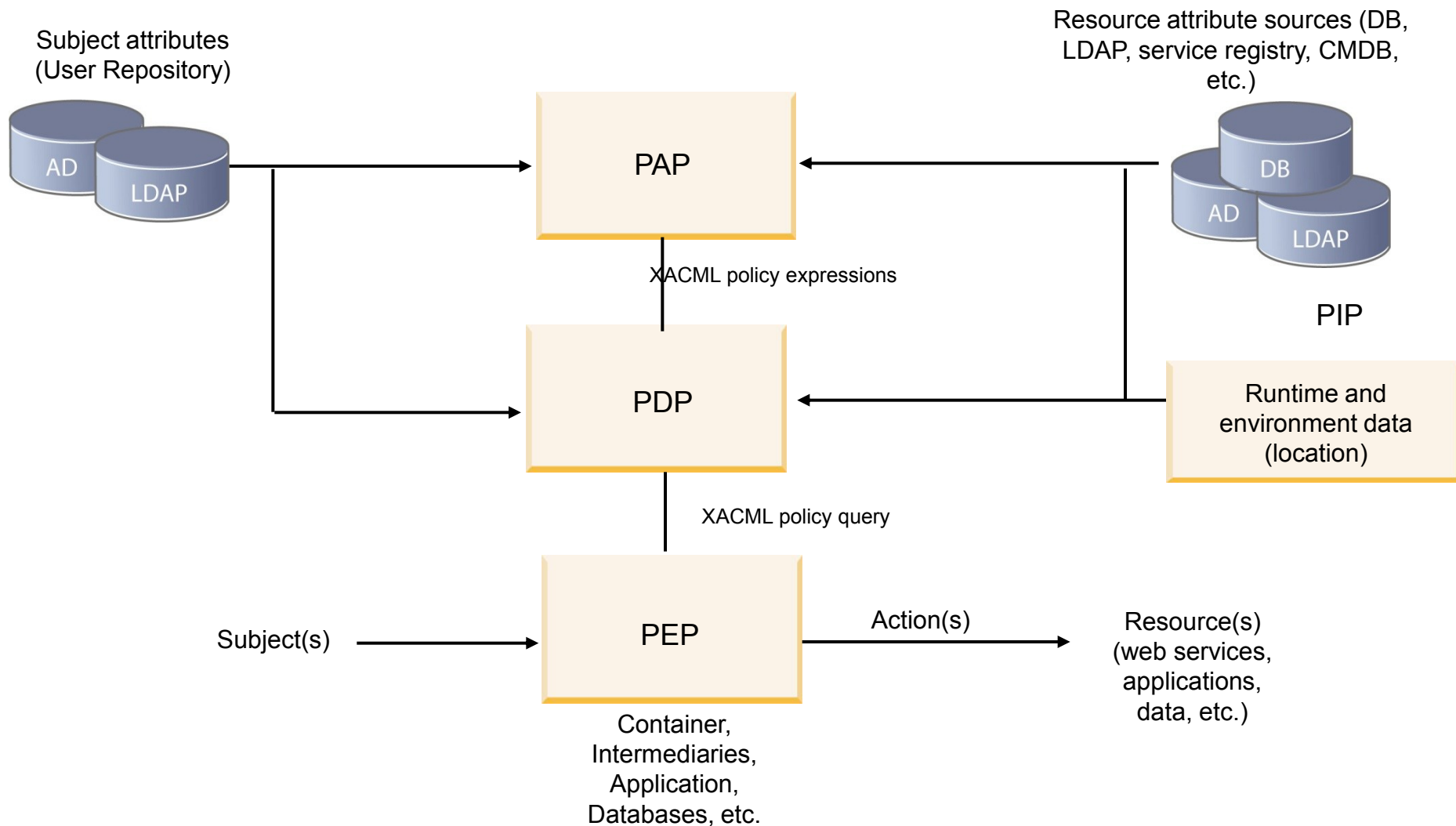
# TSPM provides the ability connect business requirements to IT



**Demonstrate Compliance and Enable Identity Governance**

# Solution Pattern – component and interactions

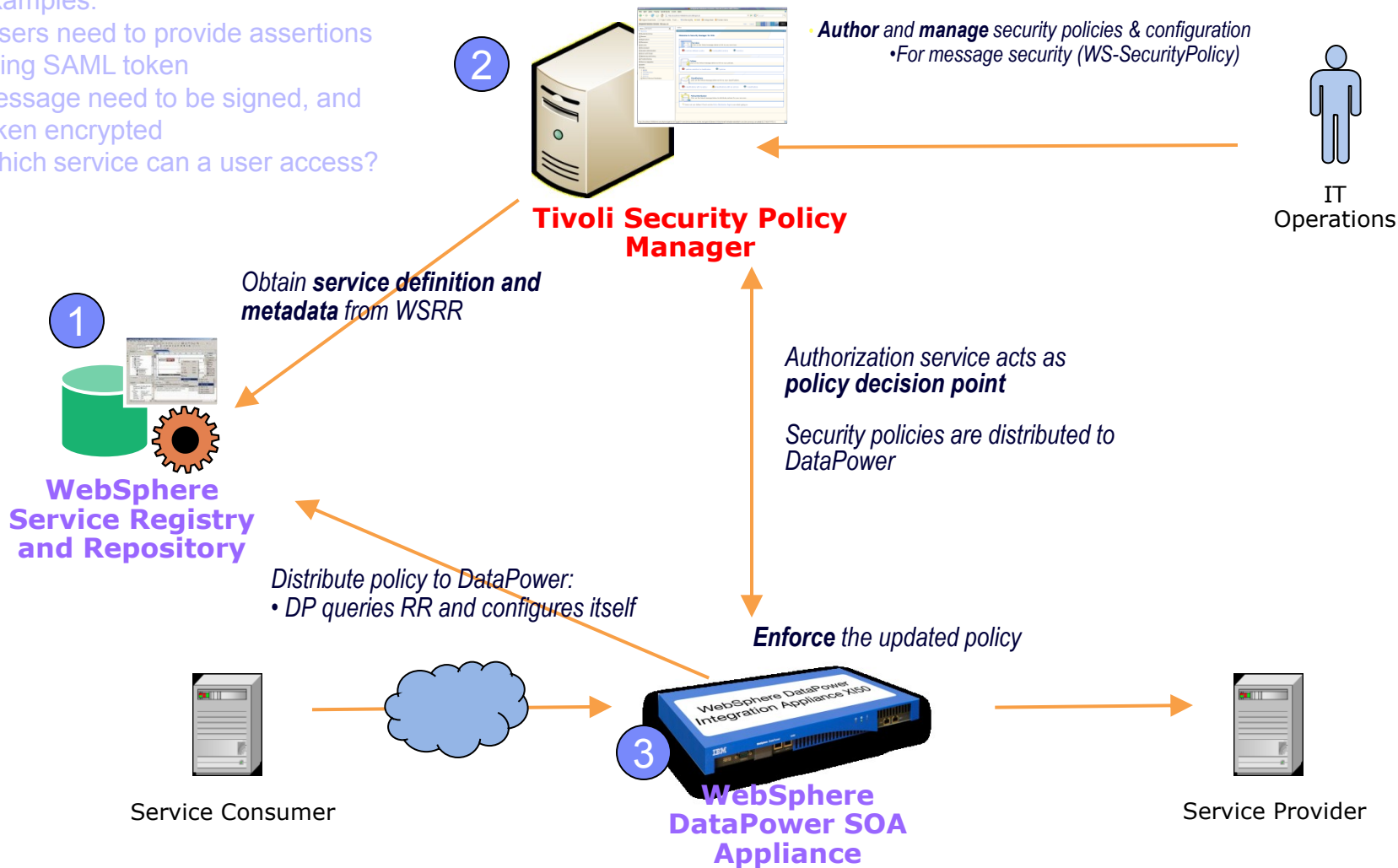
Ability to deliver end-to-end authorization



# Scenario – SOA Security Policy Management & Enforcement

Examples:

- Users need to provide assertions using SAML token
- Message need to be signed, and token encrypted
- Which service can a user access?



# Summary

- With SOA, Security is about business, no longer just about technology
- The SOA Security Reference Model provides the capabilities required for end-to-end security
- Message Protection, Identity Management and Compliance are critical components of SOA Security
- Policy is key to achieve business-to-IT alignment
  - Ability to factor business objectives into operational policy management
- Solution Approach
  - Metadata and context driven unified policy management
  - Standards based consistent security enforcement – security as a service
  - Introducing Tivoli Security Policy Manager