



# Taller en Plataforma de Interoperabilidad: Consumo de servicios

Marzo, 2015

Ignacio Friedmann  
Fernando Maidana

Arquitectura - Agesic

# Agenda

---

Plataforma de interoperabilidad

---

Principales Características y Beneficios

---

Catálogo de Servicios

---

Consumo y Publicación de servicios

---

Conclusiones

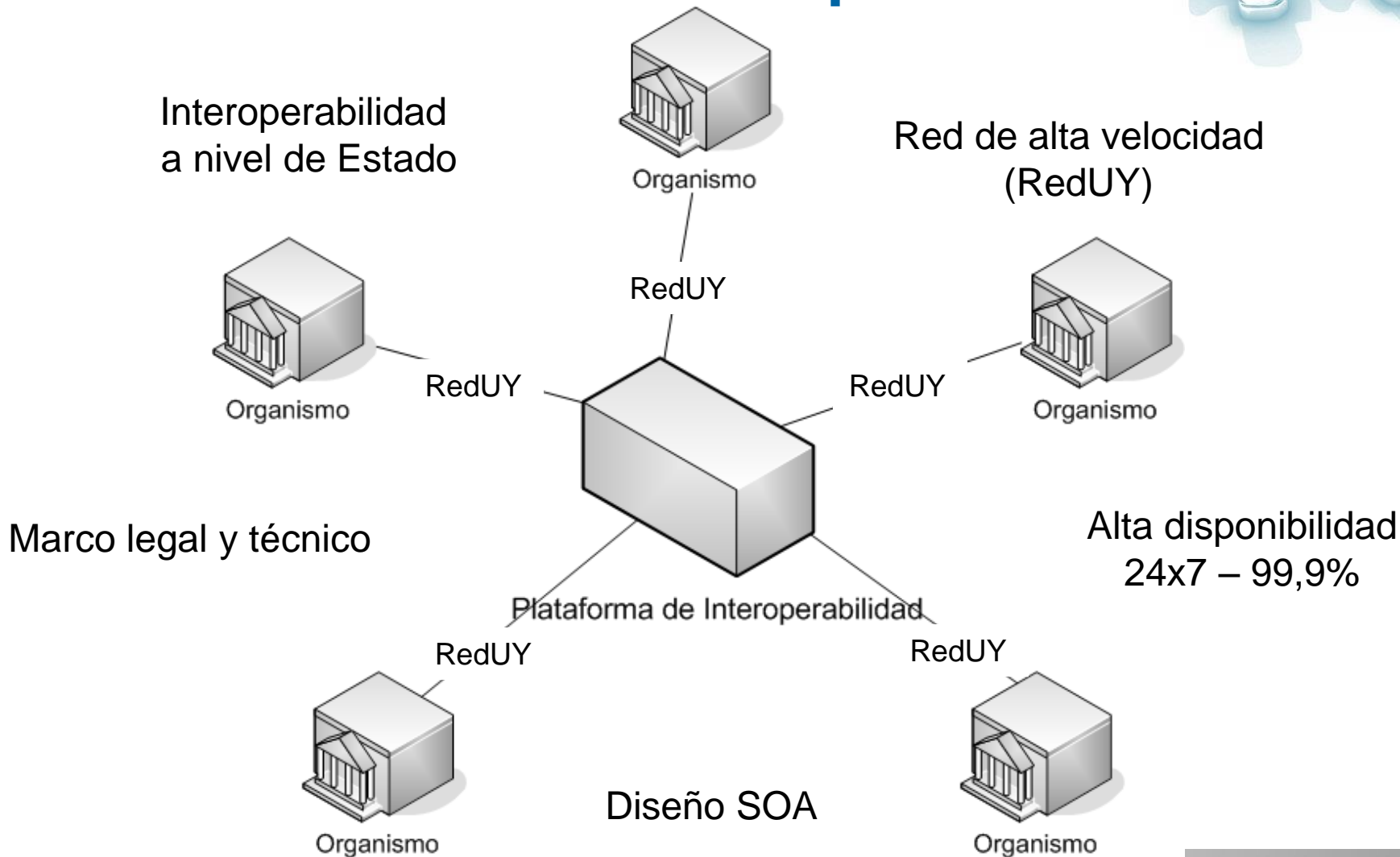
---



# Problemática

	Mecanismo de Seguridad
	Dimensionamiento de Infraestructura
	Conectividad
Intercambio de Información	Interoperabilidad técnica
	Interoperabilidad semántica
	Monitoreo
	Auditoría
	Soporte y Personal Necesario

# Plataforma de interoperabilidad



# Plataforma de interoperabilidad: Arquitectura



Organismo Proveedor



Organismo Cliente



Security Token Service  
(TFIM)



Policy Enforcement  
Point  
(Datapower)



ESB



Policy Decision Point  
(TSPM)

Plataforma de interoperabilidad

# Principales beneficios



## Estandarización

- Seguridad
- Protocolos
- Semántica
- Operativa
- Gobernanza

## Reducción de costos

- Economías de escala

## Diseño SOA

- Reutilización de servicios
- Arquitectura flexible
- Integración con sistemas legados

# Principales características



---

Servicio de Control de Acceso

---

Servicio de Ruteo

---

Servicio de novedades

---

Servicio de administración y control de carga

---

Servicio Conector PGE

---

Servicio Interfaces Web

---

Servicio de reportes estadísticos

---

Servicio de monitoreo

---

Servicio de metadatos

---

# Principales características



Servicio de Control de Acceso

Servicio de Ruteo

Servicio de novedades

Servicio de administración y control de carga

Servicio Conector PGE

Servicio Interfaces Web

Servicio de reportes estadísticos

Servicio de monitoreo

Servicio de metadatos



# Catálogo de servicios



Servicio básico de información  
Servicio CI Digital  
Consulta de Datos Infantes



Remuneraciones del contribuyente  
Verificación de actividad  
Empresas por contribuyente



Comprobante de Nacido Vivo  
Certificado de defunción



Certificado de vigencia anual  
Información del contribuyente



Permisos de importación y  
exportación de automóviles



# Catalogo de servicios



The screenshot shows a Google search interface. The search bar contains the text 'catalogo servicios agestic'. Below the search bar, the results are displayed. The first result is highlighted with a green arrow pointing to it from the right. The results include:

- Web** Imágenes Videos Más ▾ Herramientas de búsqueda
- Cerca de 35.000 resultados (0,29 segundos)
- [AGESIC - Catálogo de Servicios - Agestic - Portal del Estado Uruguayo](#)**  
[www.agesic.gub.uy/.../agesic/catalogo\\_de\\_servicios.html?...](#)  
Empresa - Contribuyente - Aportación. Permite saber si la relación entre la empresa y el contribuyente; y la relación entre la empresa y la aportación, es válida ...
- [AGESIC - Disponible Catálogo de artículos, servicios y obras que ...](#)**  
[www.agesic.gub.uy > ... > Noticias de Gobierno en red](#)  
28/06/2011 – Disponible **Catálogo** de artículos, **servicios** y obras que utiliza el Estado. **AGESIC** puso a disposición en [comprasestatales.gub.uy](#) y en el ...
- [AGESIC - Página principal del Sitio](#)**  
[www.agesic.gub.uy/](#)  
Logo de **AGESIC** - Logo de la Presidencia de la República Oriental del Uruguay ...  
**Catálogo** de Datos Abiertos · UCE: convocatoria a prestadores de **servicios** ...  
Visitaste esta página 4 veces. Última visita: 19/11/12

# Clientes sobre la Plataforma



La energía que nos une



MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS



# Consumo de servicios

- Comprender
  - Mecanismos de seguridad (Servicio de seguridad)
  - Mecanismos de ruteo (Servicio de Ruteo)
- Resultados
  - Auditoría
  - Registro de consumo

# Servicio de Seguridad



- Aplicación de políticas AAA de seguridad
  - Autenticación, Autorización y Auditoría
- Garantizar no repudio de transacciones
- Prevención de ataques de seguridad
  - Denial of Service (DoS), SQL Injection, etc

# Servicio de Seguridad



- Autenticación
  - Modelo basado en confianza
  - WS-Trust, SAML, Certificados (Persona Jurídica)
- Autorización
  - Modelo basado en RBAC
- Auditoría
  - Quién consumió? Qué servicio? Cuándo?

# Autenticación



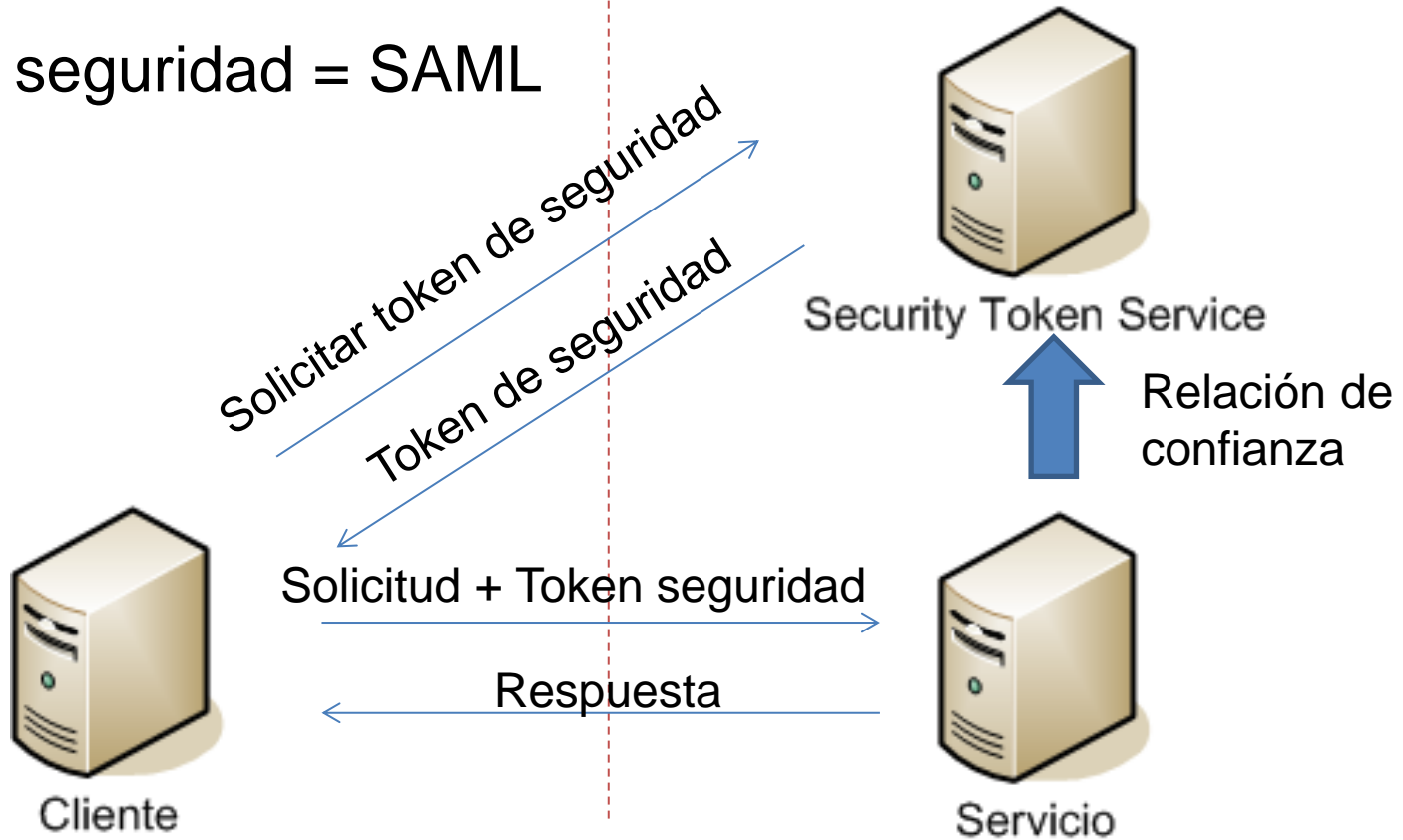
- Autenticación basada en confianza
  - Aplicación del estándar WS-Trust + SAML
  - No hay autenticación de usuarios, sí de organismos
- WS-Trust
  - Estándar para autenticación de Web Services en ambientes federados
- SAML
  - Estándar que define entre otras cosas un formato de credenciales basado en XML

# WS-Trust + SAML

Organización A

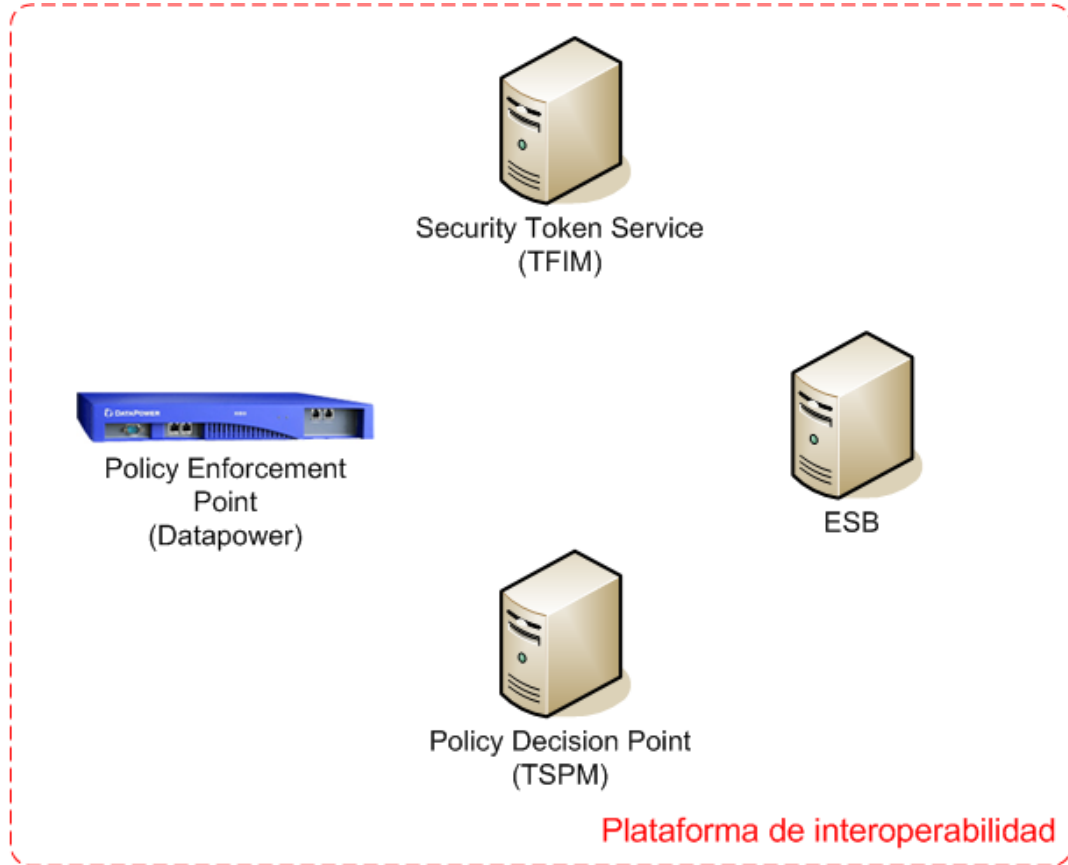
Organización B

Token de seguridad = SAML

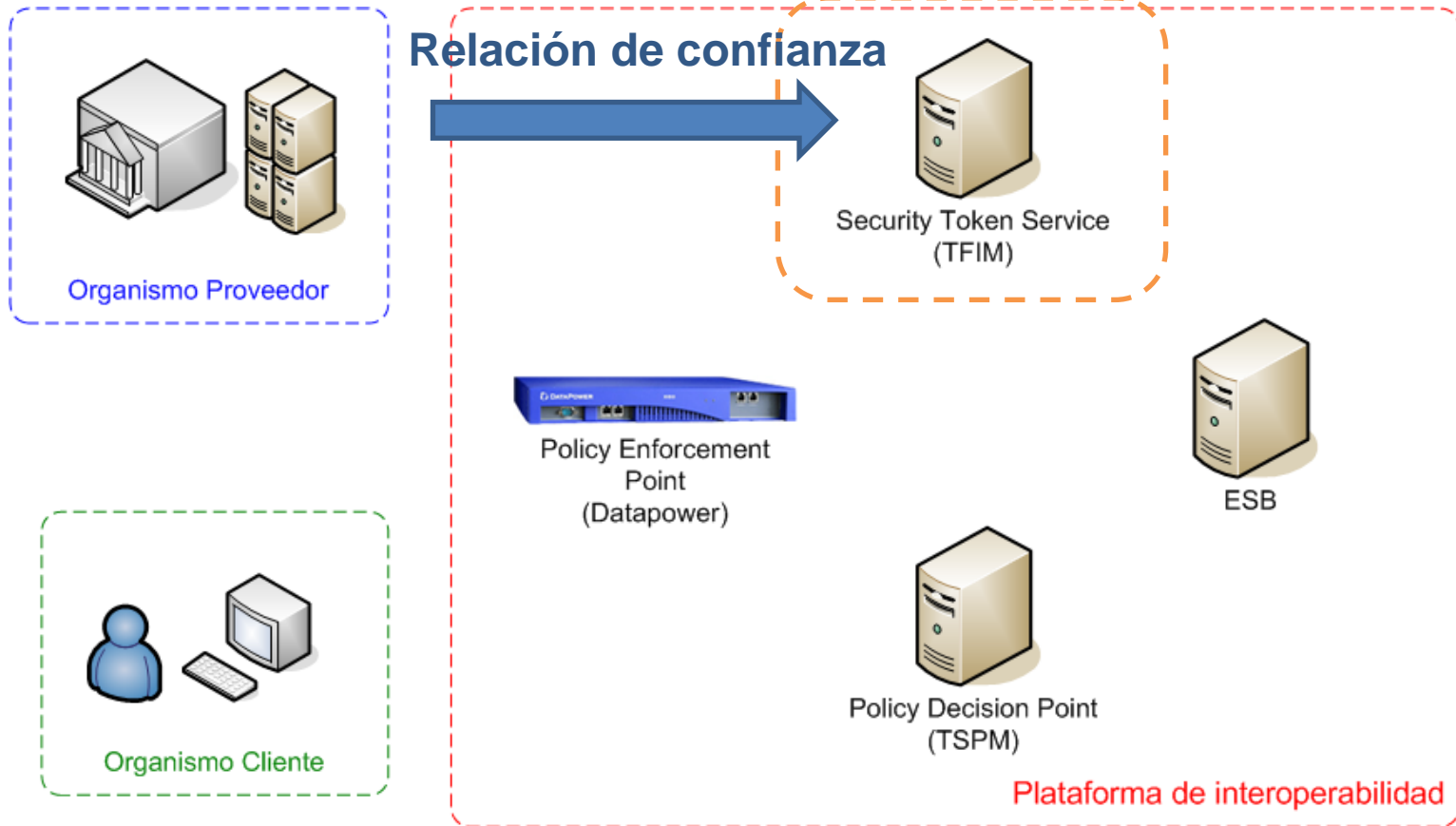




# Autenticación en Plataforma



# Autenticación en Plataforma



# Autenticación en Plataforma



## Mensaje para el STS

- Servicio a consumir
- Token SAML
  - Rol del usuario
  - Usuario
  - Firma de org.



Organismo Cliente



Policy Enforcement Point  
(Datapower)



Security Token Service  
(TFIM)



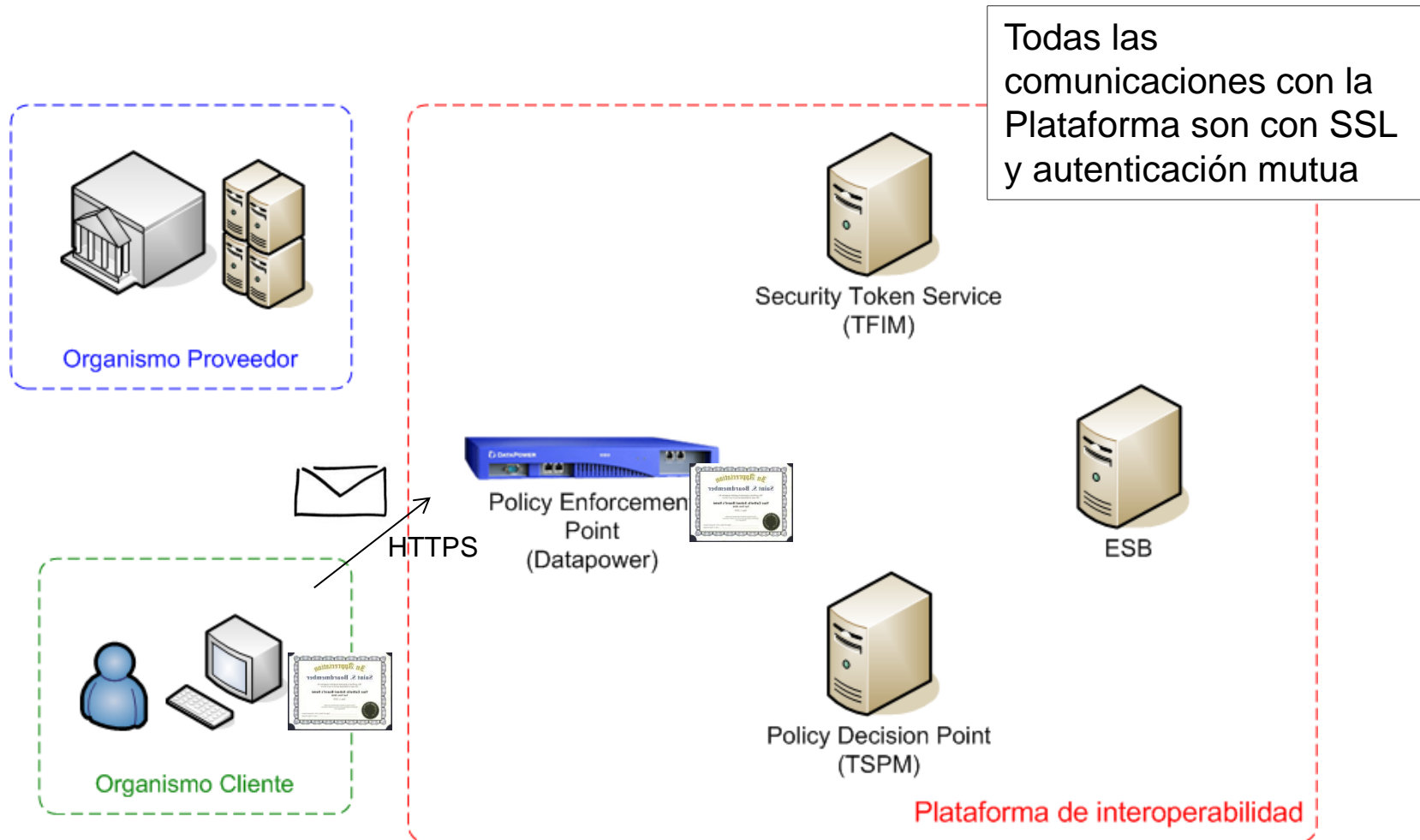
ESB



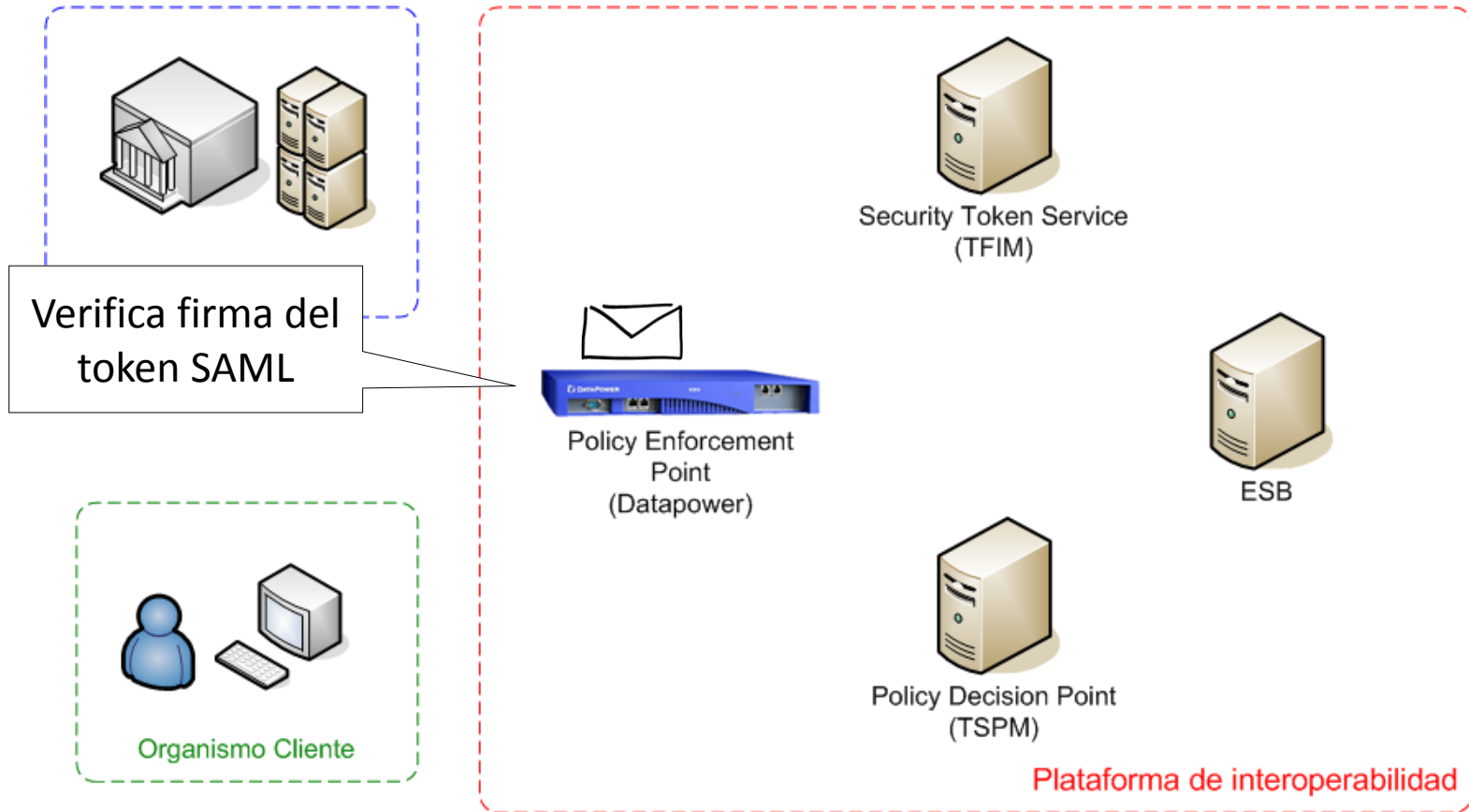
Policy Decision Point  
(TSPM)

Plataforma de interoperabilidad

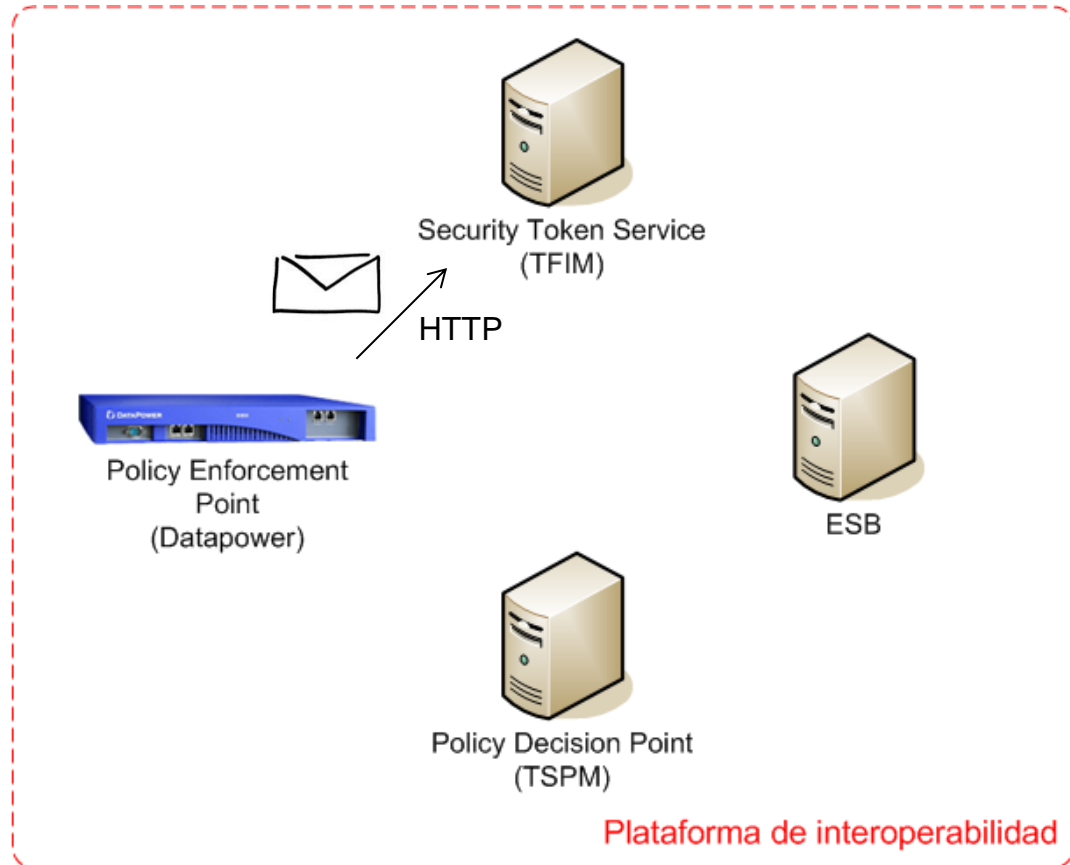
# Autenticación en Plataforma



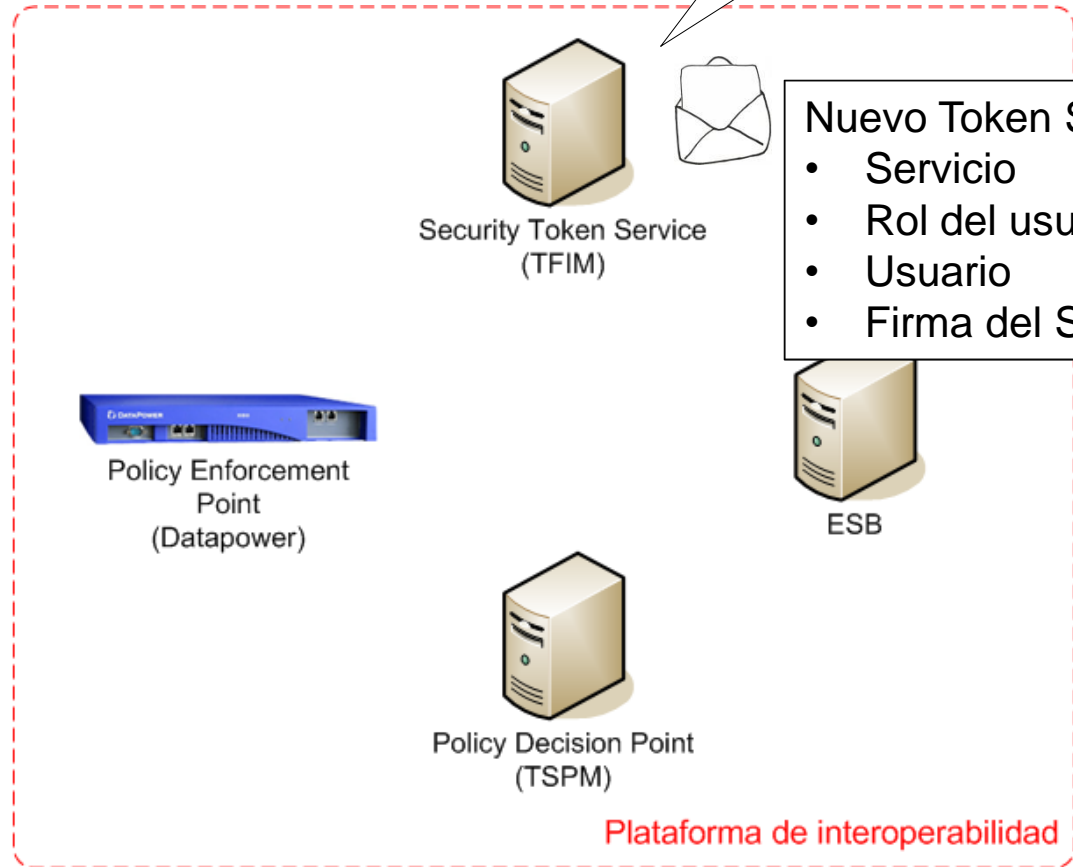
# Autenticación en Plataforma



# Autenticación en Plataforma



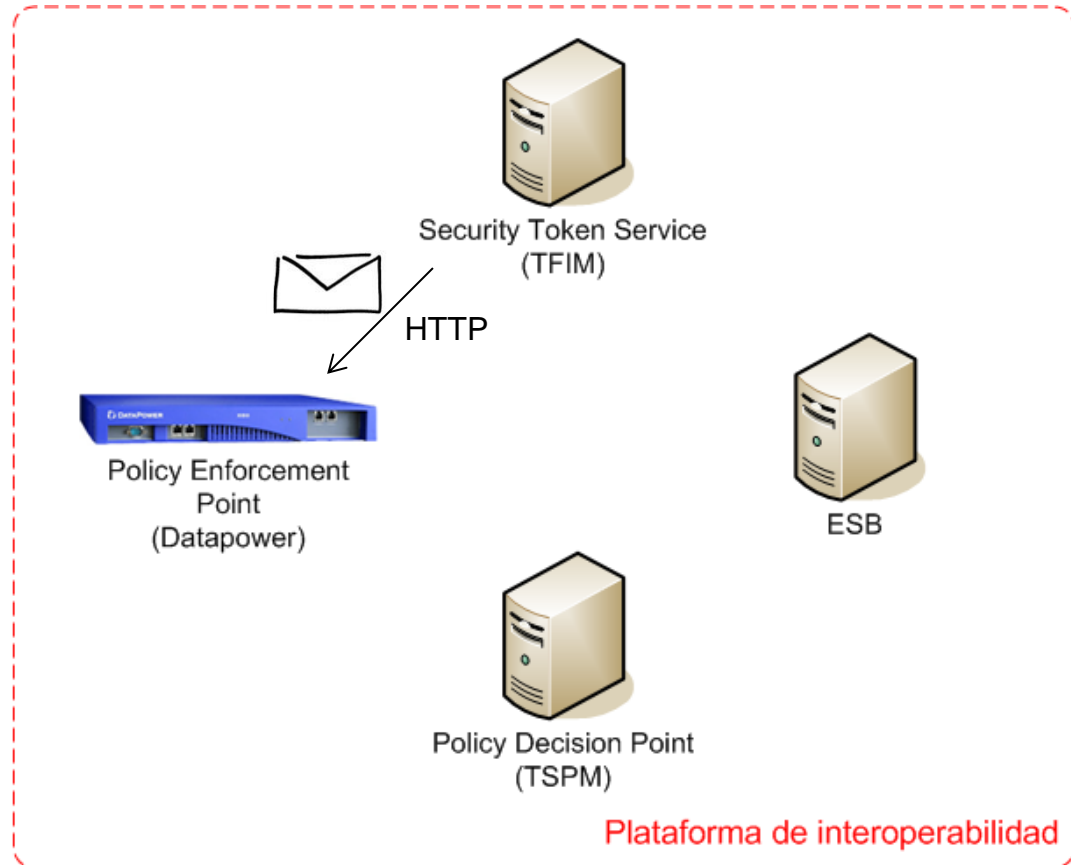
# Autenticación en Platafo



Emite nuevo token SAML

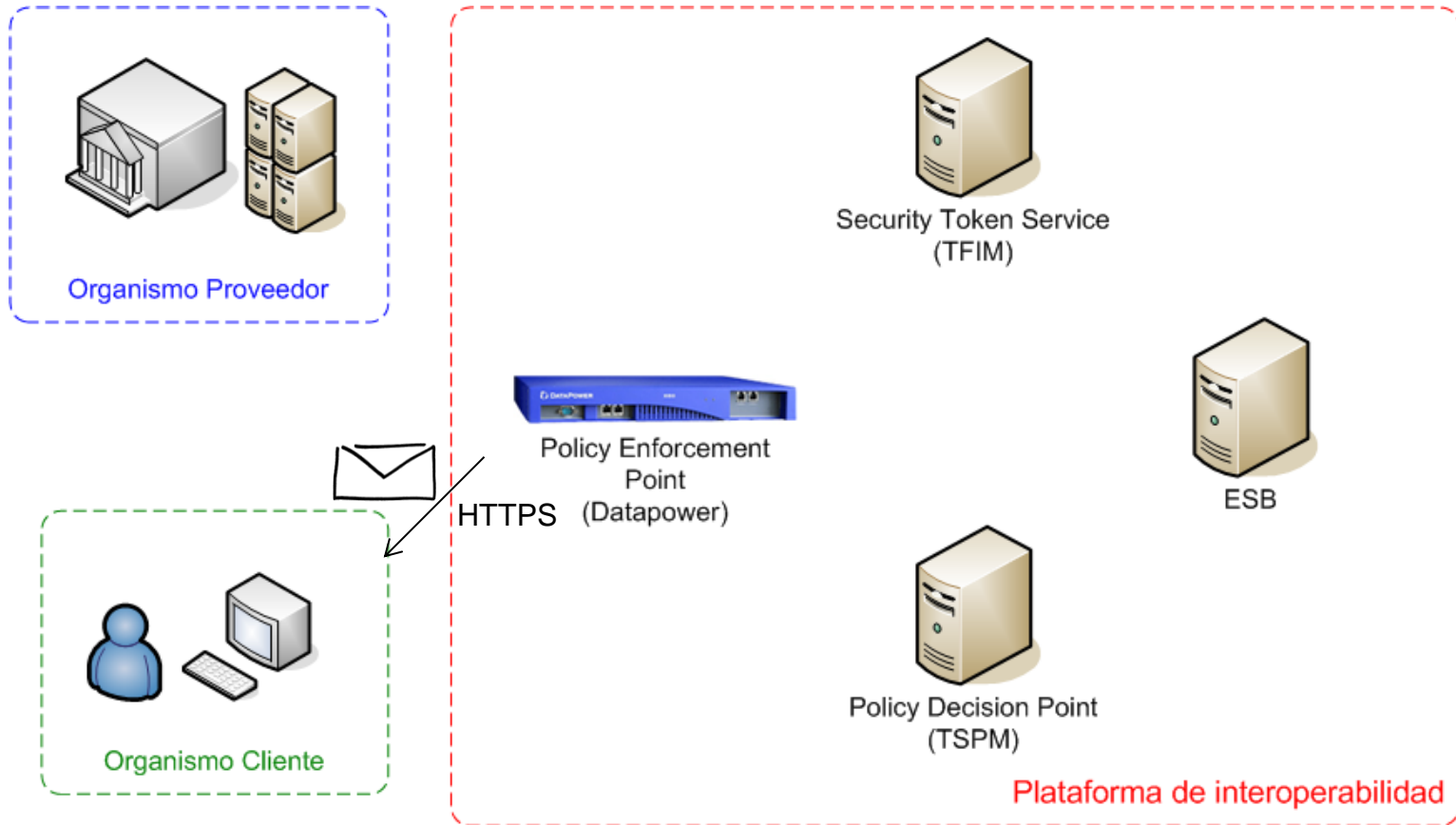
- Nuevo Token SAML
- Servicio
  - Rol del usuario
  - Usuario
  - Firma del STS

# Autenticación en Plataforma





# Autenticación en Plataforma



# SAML en Plataforma

## SAML emitido por Cliente

Rol del Cliente

Usuario del Cliente

Firma del Organismo

Servicio a Consumir

## SAML emitido por STS

Rol del Cliente

Usuario del Cliente

Firma del Organismo

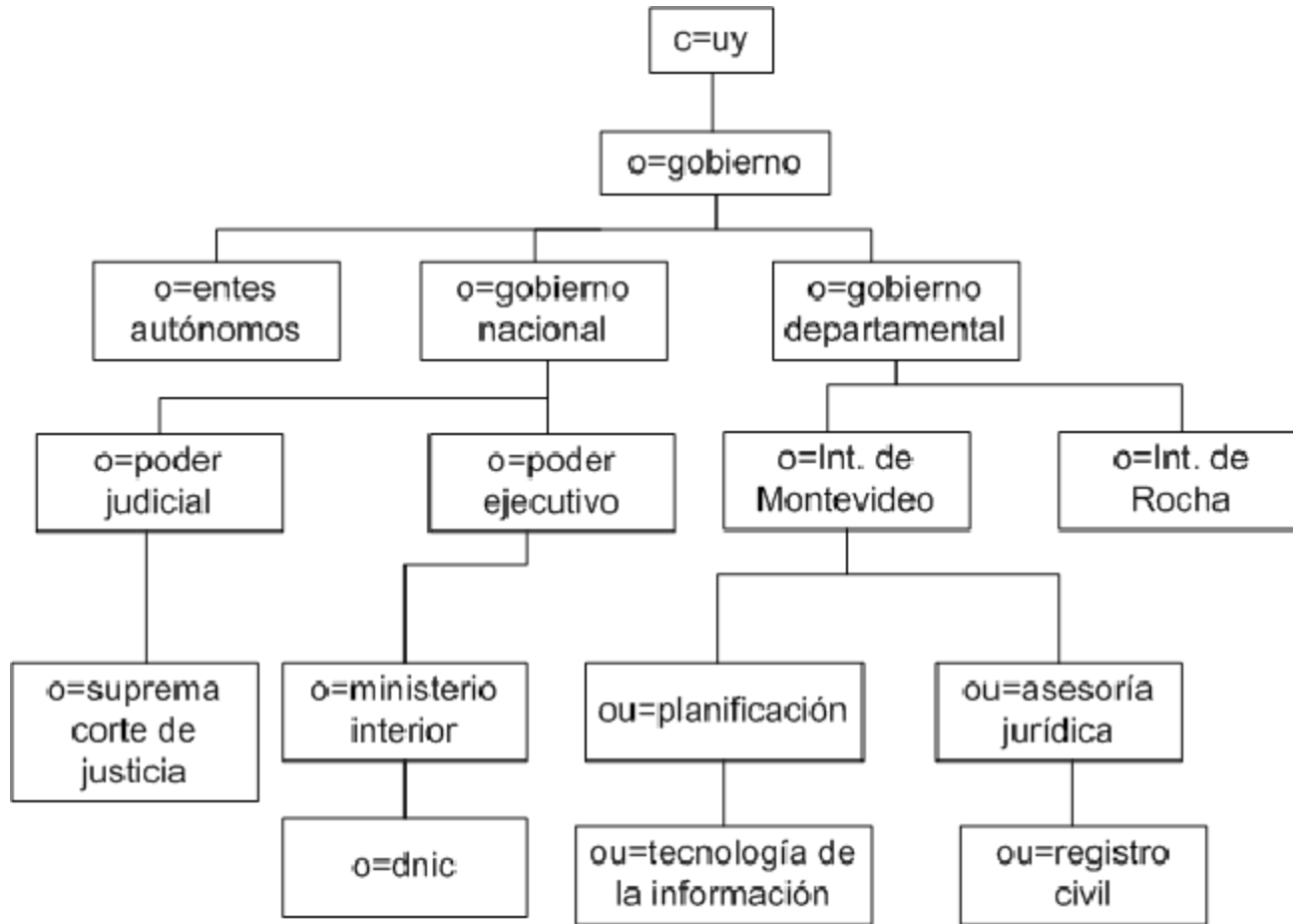
Servicio a Consumir

Firma del STS

# Autorización

- Autorización basada en roles similar a RBAC
  - Roles a nivel de sección de organización o aplicación
    - Ej1: Secretaría General del Ministerio del Interior
    - Ej2: Sistema de Gestión de Registro de Estado Civil (SGREC)
  - Granularidad a nivel de método del Web Service
    - Un rol puede consumir un método X del WS
- Permiso de roles denegado por defecto
- Jerarquía de roles con herencia de permisos descendente

# Jerarquía de roles



# Autorización en Plataforma



Organismo Proveedor



Organismo Cliente



Security Token Service  
(TFIM)



Policy Enforcement  
Point  
(Datapower)



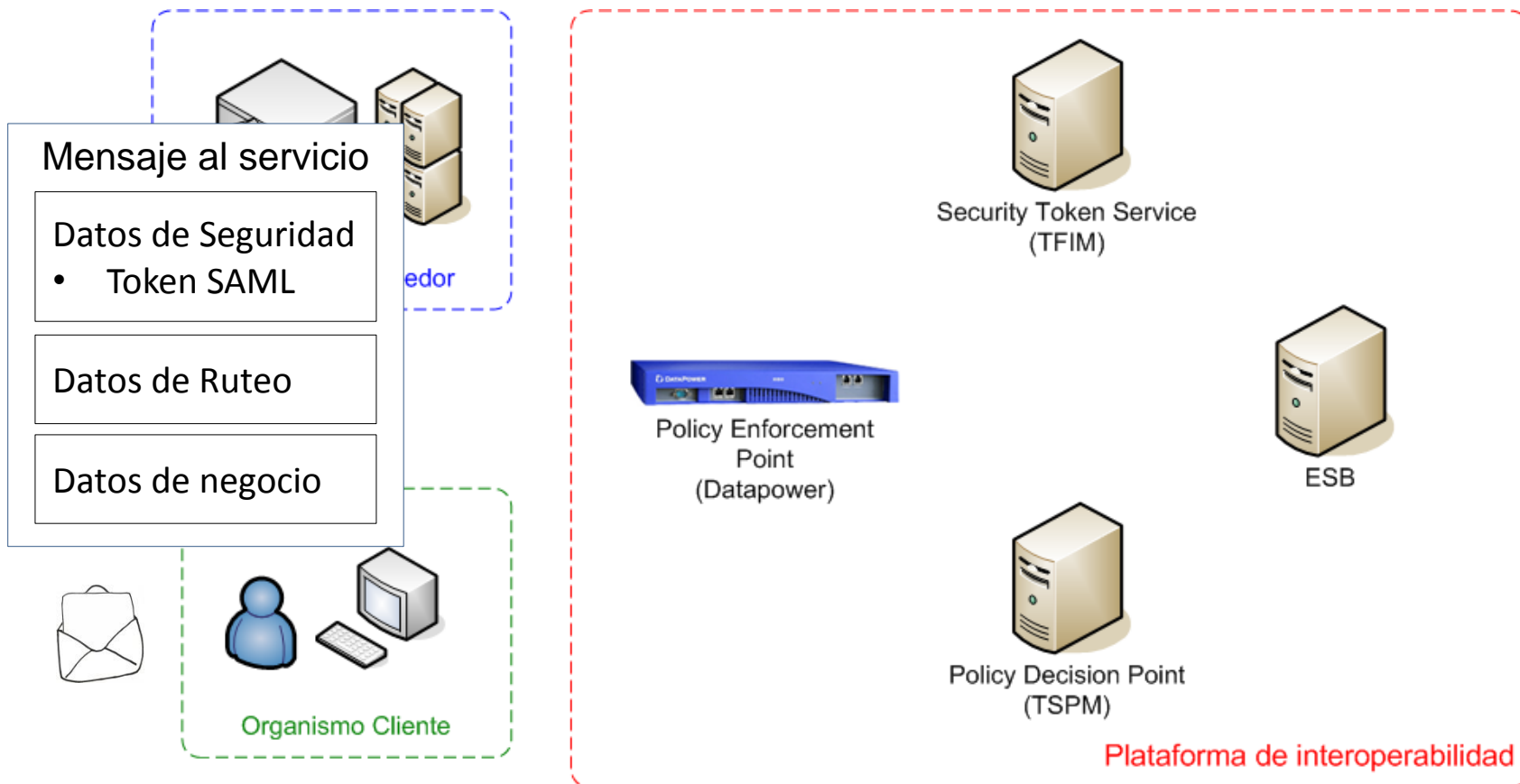
ESB



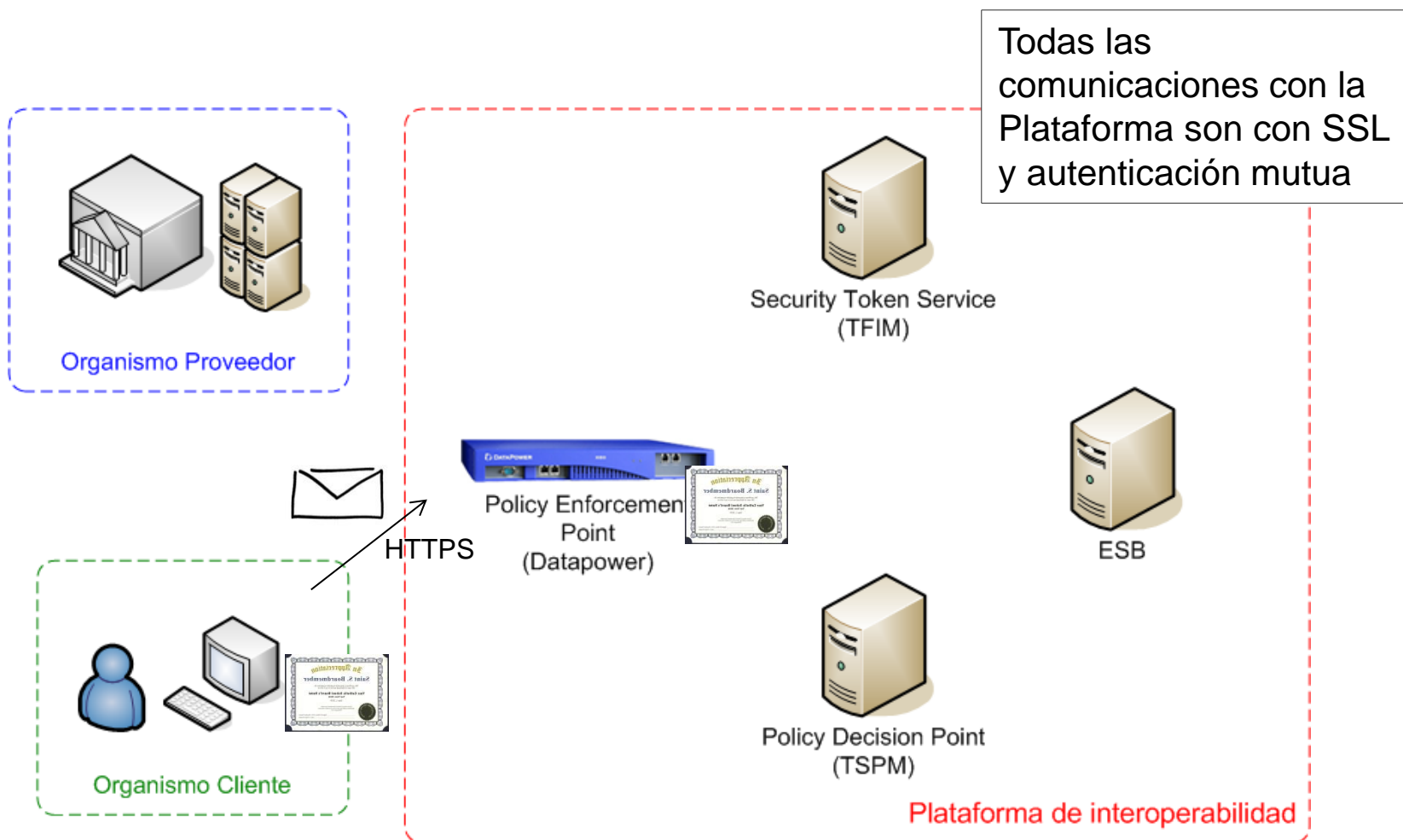
Policy Decision Point  
(TSPM)

Plataforma de interoperabilidad

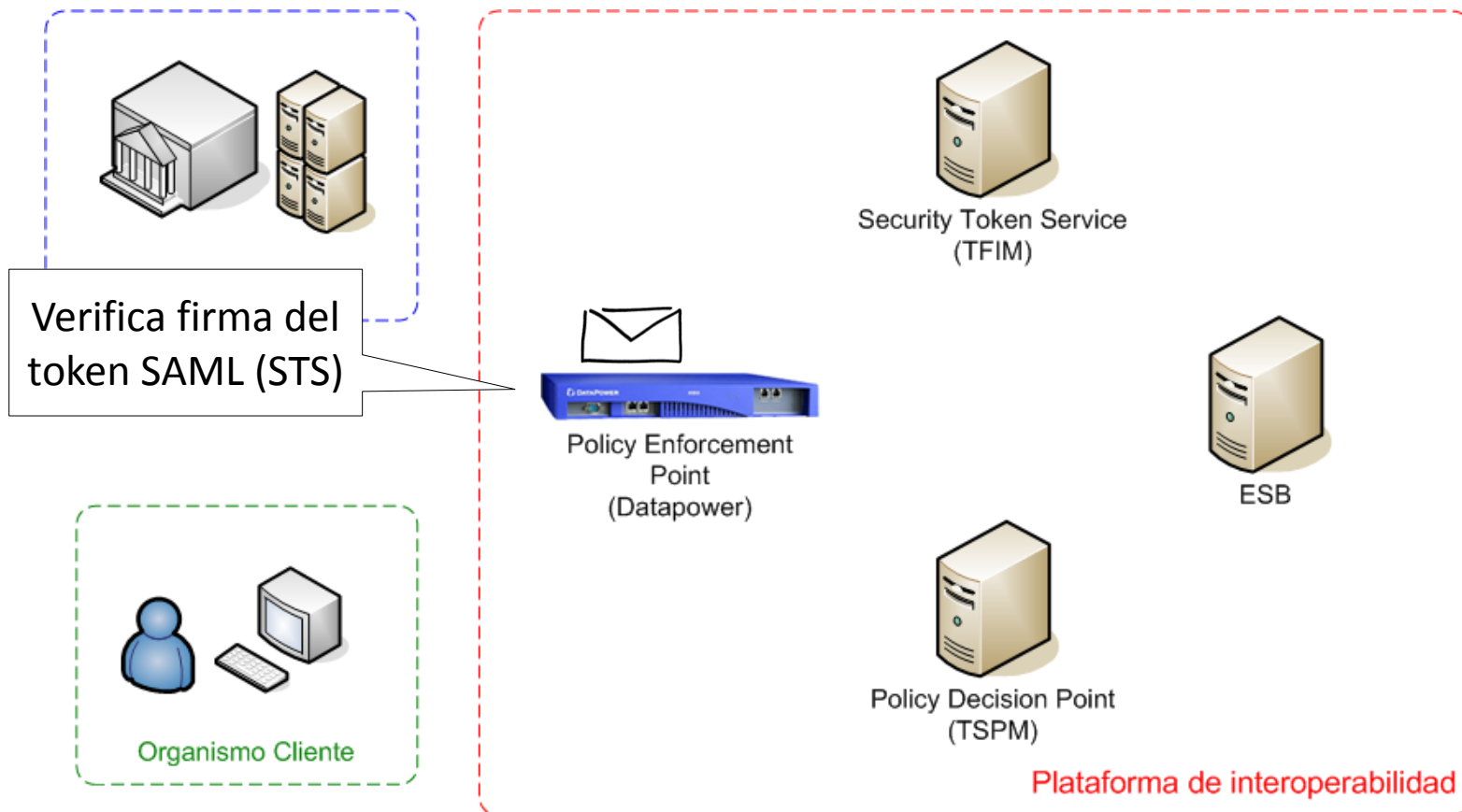
# Autorización en Plataforma



# Autorización en Plataforma

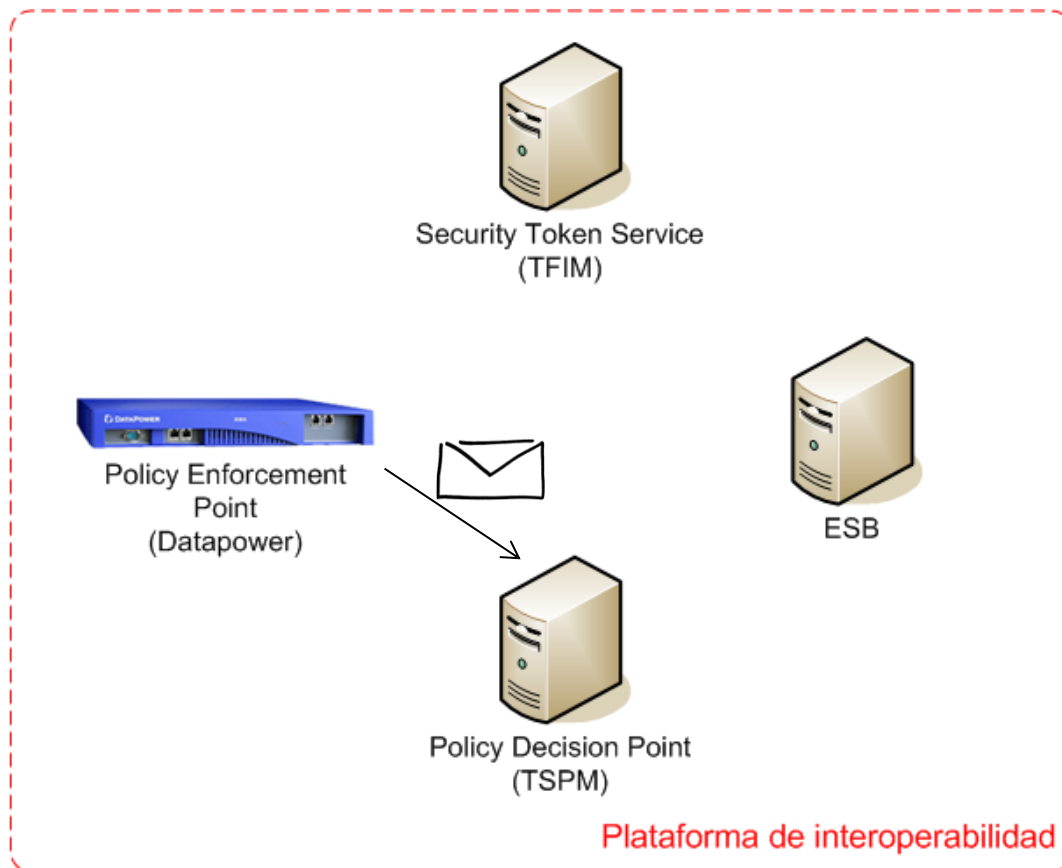


# Autorización en Plataforma

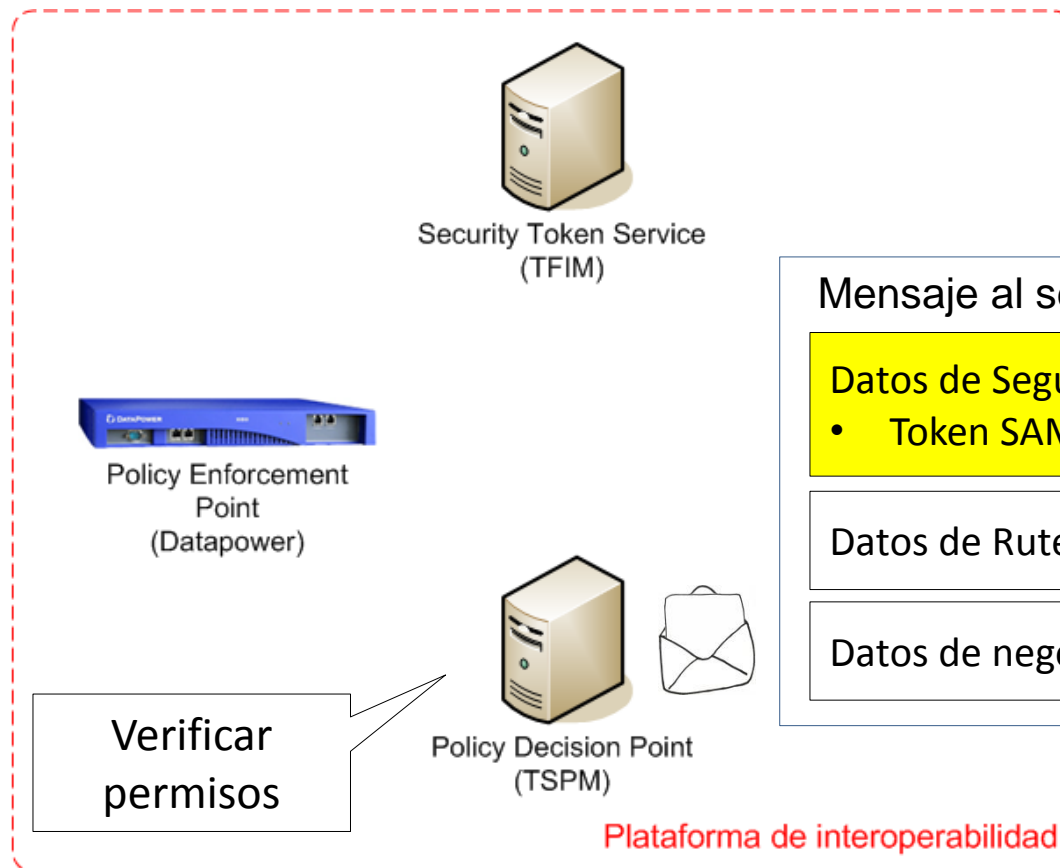




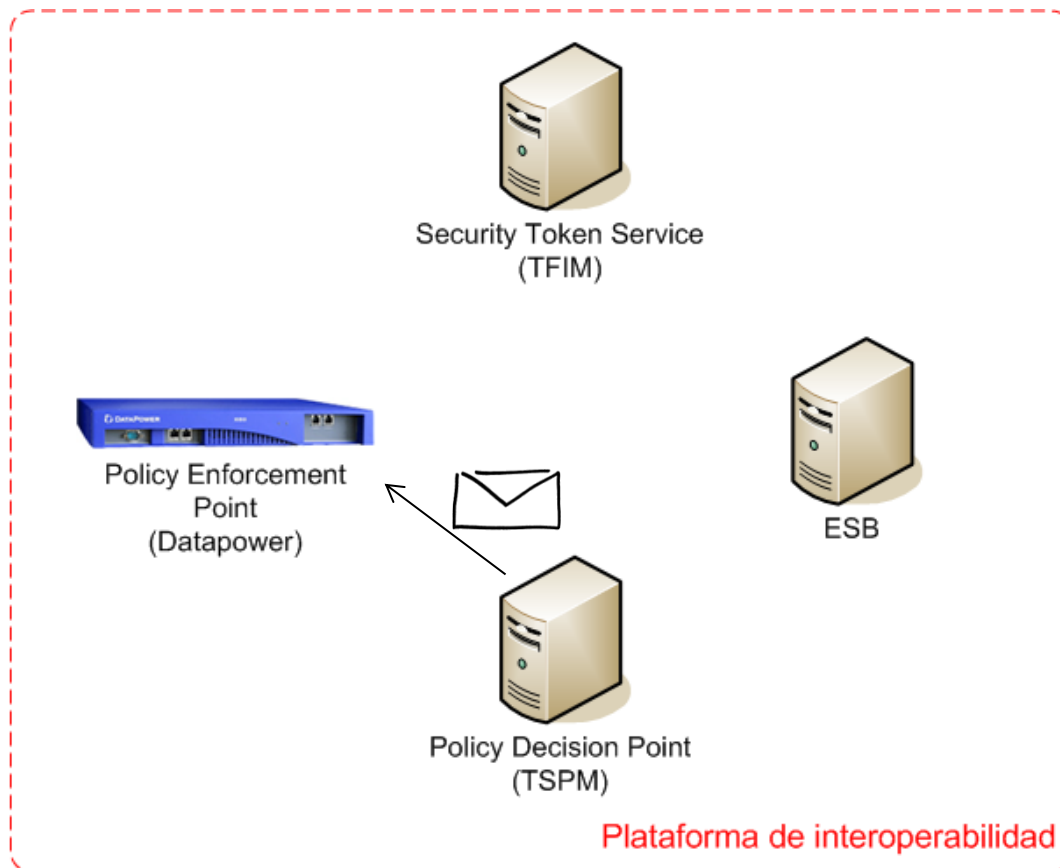
# Autorización en Plataforma



# Autorización en Plataforma



# Autorización en Plataforma



# Autorización en Plataforma



Organismo Proveedor



Organismo Cliente



Security Token Service  
(TFIM)



Policy Enforcement  
Point  
(Datapower)



ESB



Policy Decision Point  
(TSPM)

Plataforma de interoperabilidad

# Auditoría



- Todas las transacciones llevadas a cabo por la Plataforma se encuentra auditadas
  - ¿Quién consume?
  - ¿Qué servicio?
  - ¿A qué fecha/hora?

# Certificados

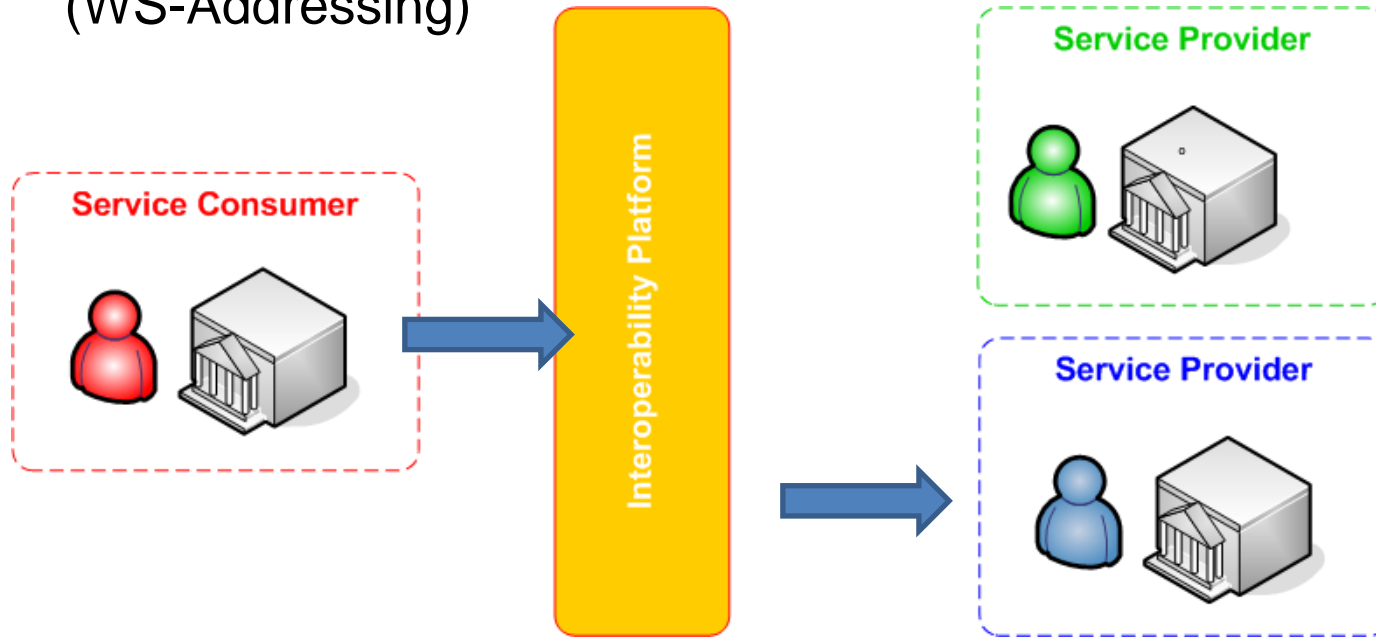


- Infraestructura:
  - SSL + Autenticación Mutua
  - Emitido por la CA de la Plataforma
  - Sin costo y duración 1 año
  - Solicitud: soporte@agesic.gub.uy
- Persona Jurídica:
  - Firma de las transacciones (Marco Legal)
  - Emitido por el Correo
  - Con costo de 100 U\$S aprox y duración 1 año
  - Solicitud: procedimientos del correo en [www.correo.com.uy](http://www.correo.com.uy)

# Servicio de ruteo



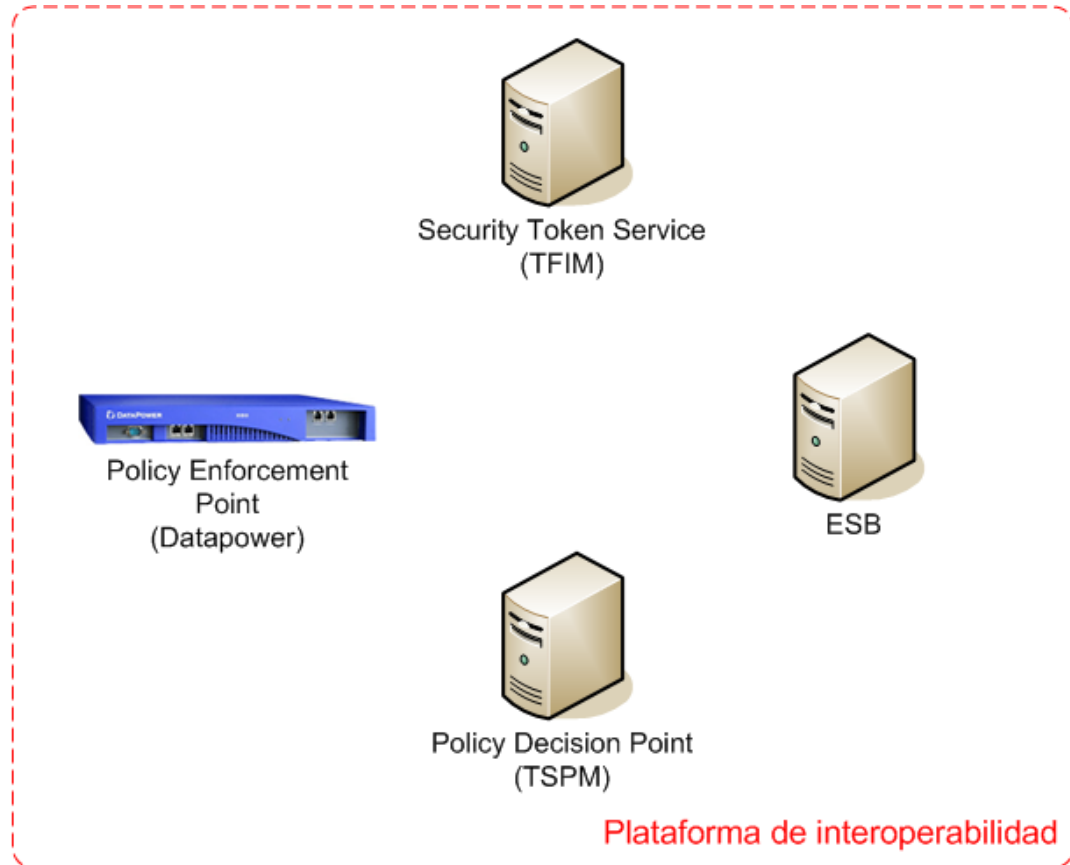
Ruteo **basado en Contenido**  
(WS-Addressing)



**Manejo avanzado de errores**  
Reconfiguración dinámica

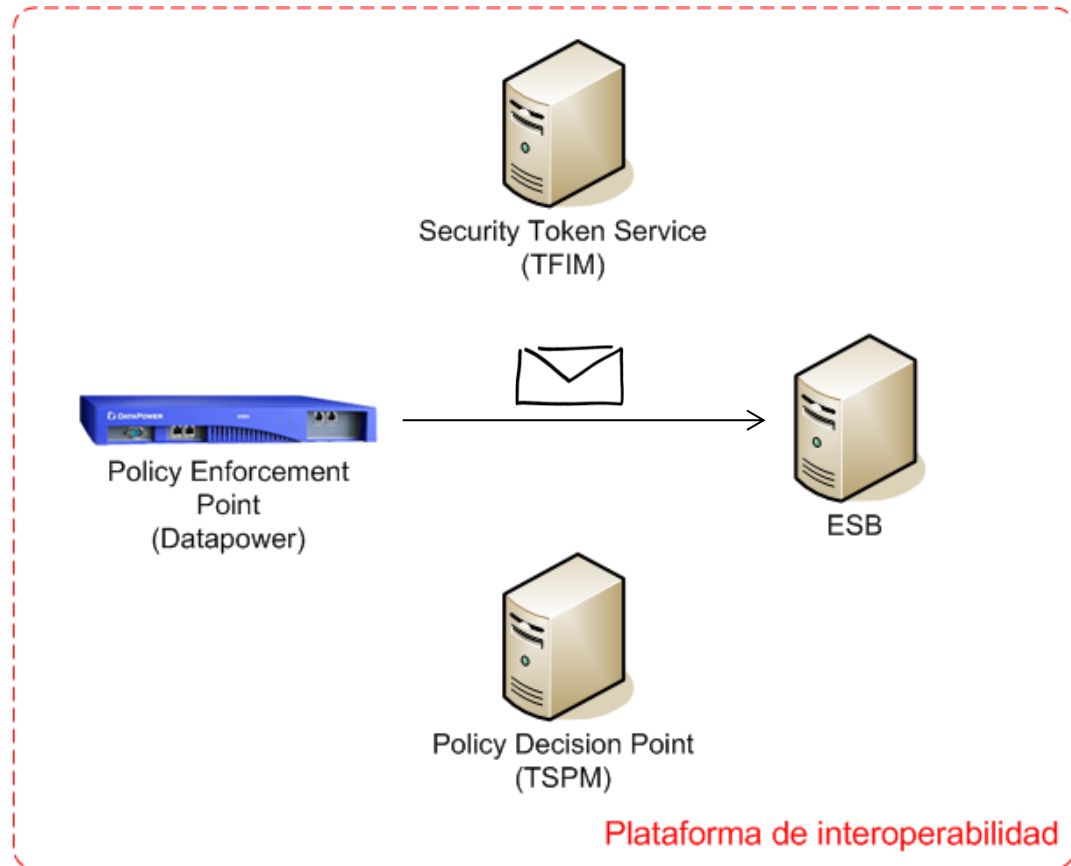
**Filtrado y transformación**  
de mensajes

# Ruteo de mensajes en Plataforma

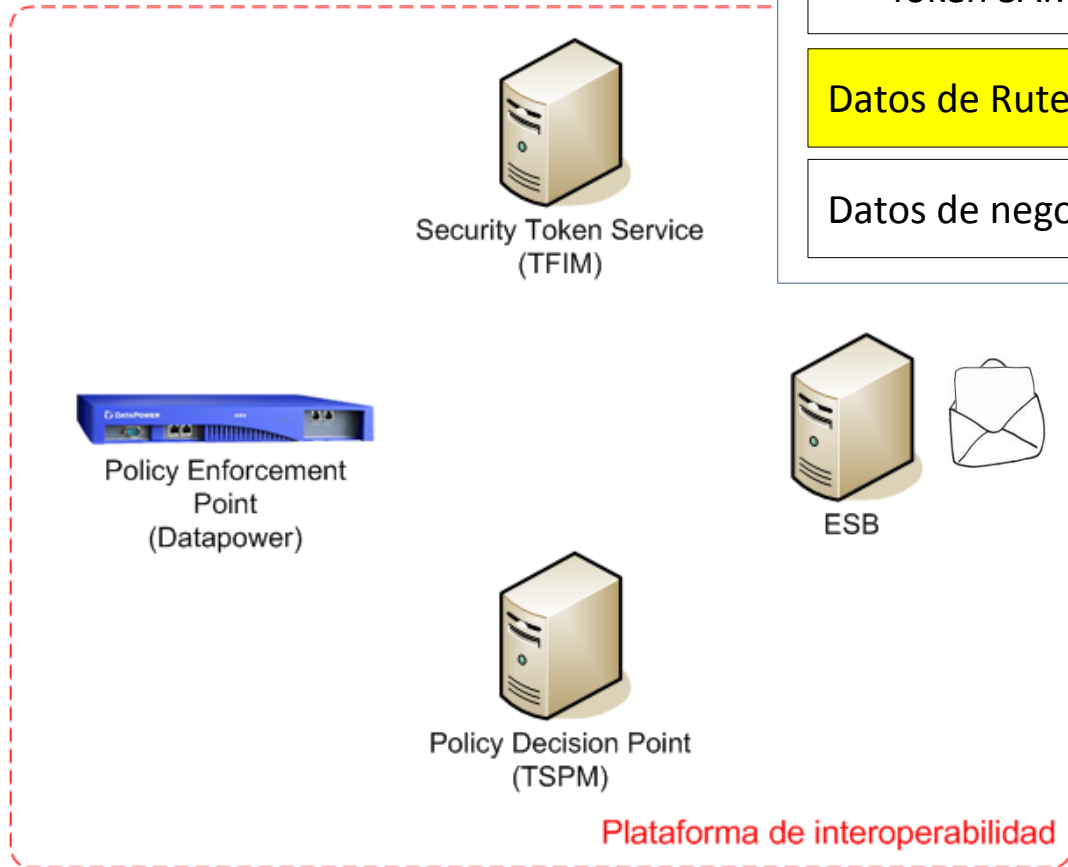




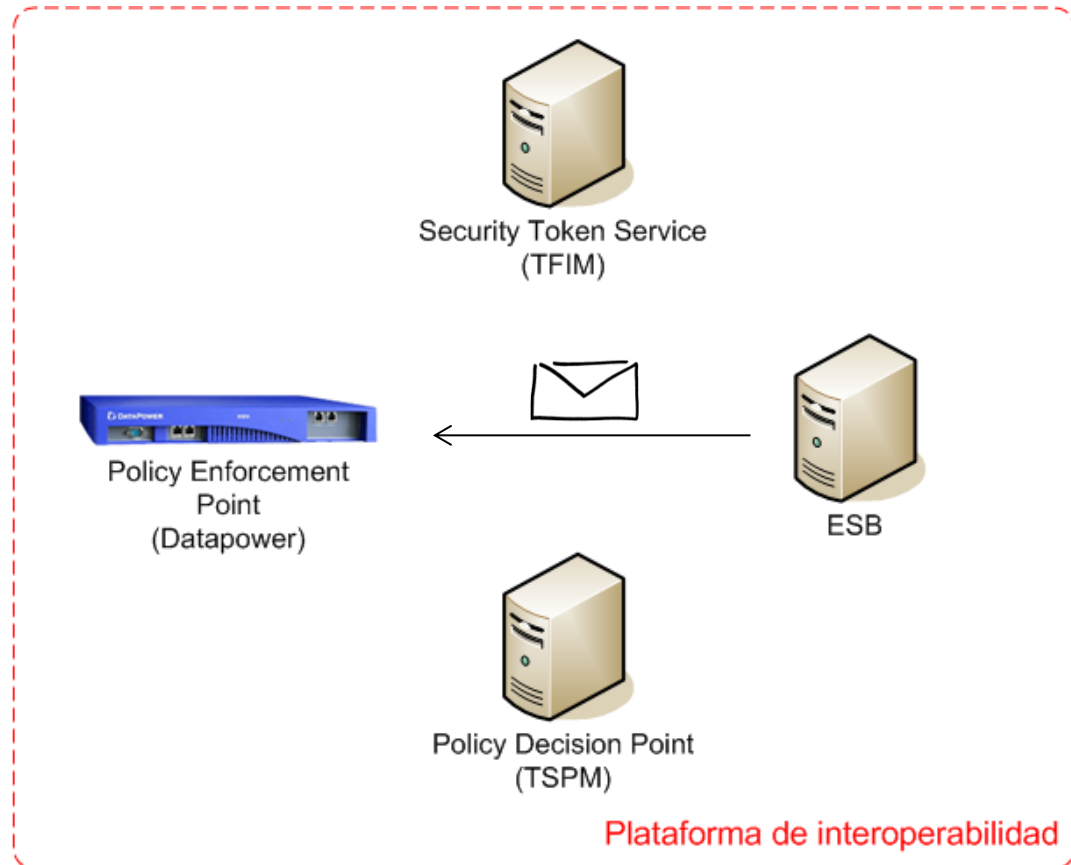
# Ruteo de mensajes en Plataforma



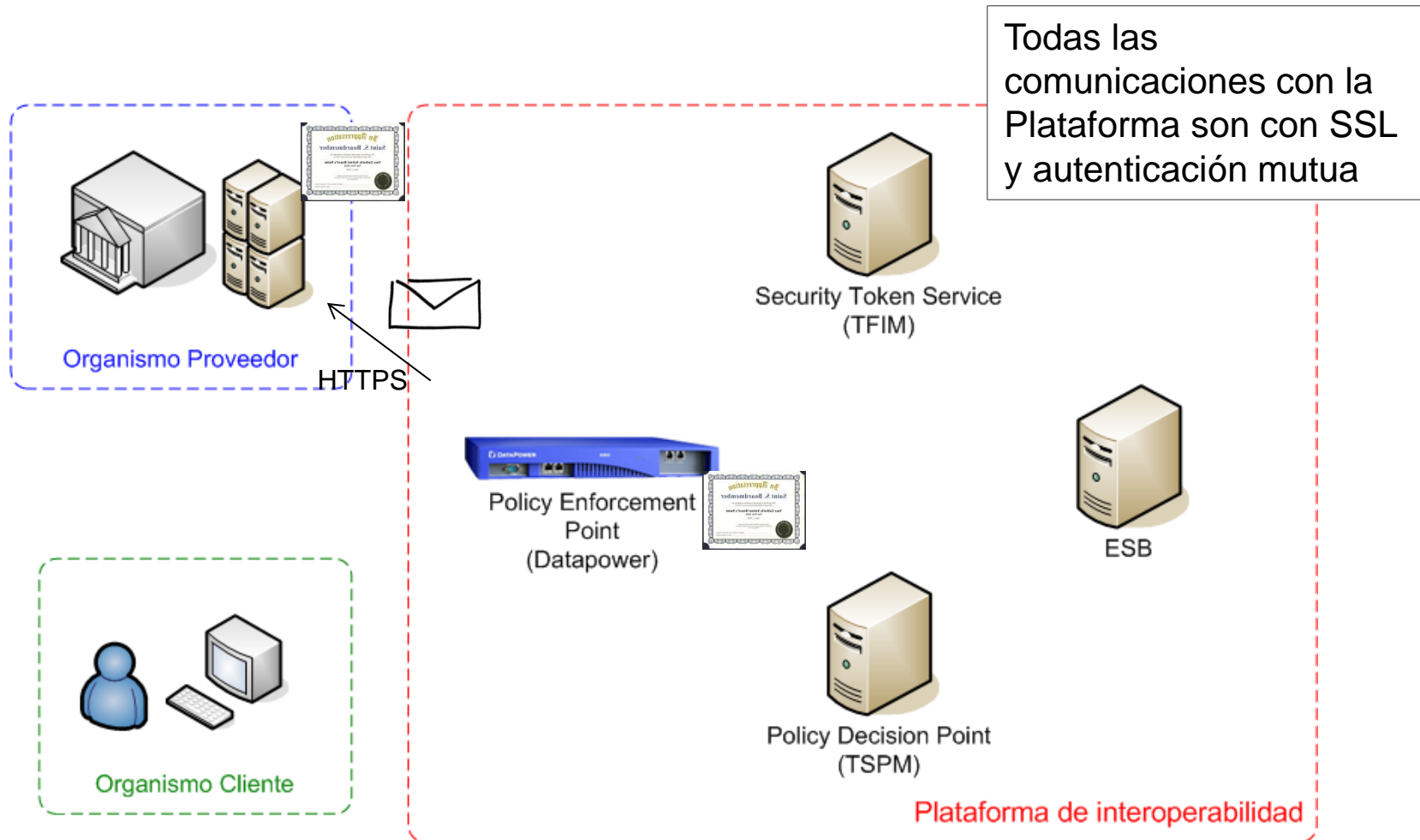
# Ruteo de mensajes en Plataformas



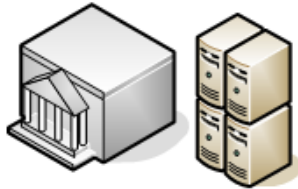
# Ruteo de mensajes en Plataforma



# Ruteo de mensajes en Plataforma



# Ruteo de mensajes en Plataforma



Organismo Proveedor



Organismo Cliente



Security Token Service (TFIM)



Policy Enforcement Point (Datapower)



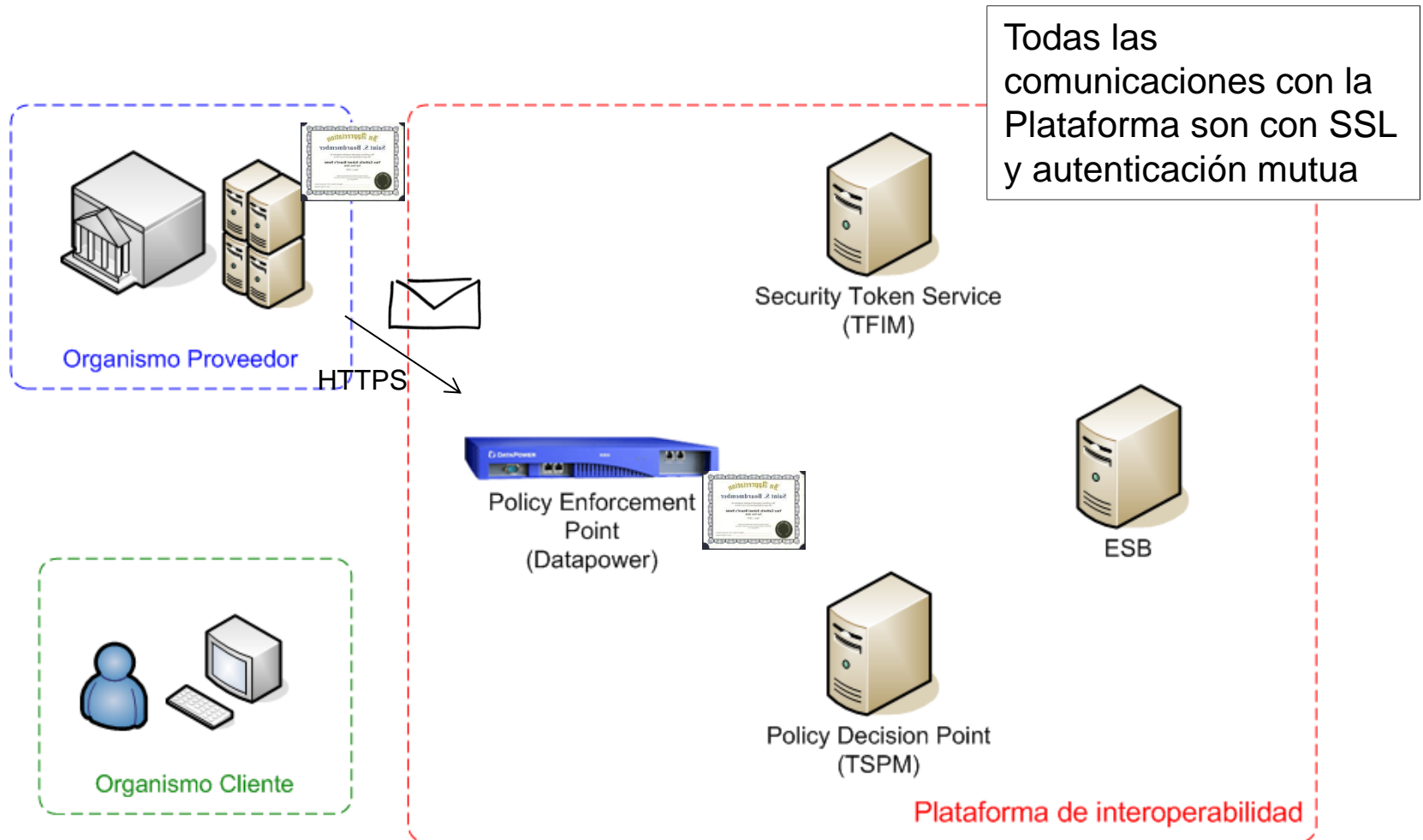
ESB



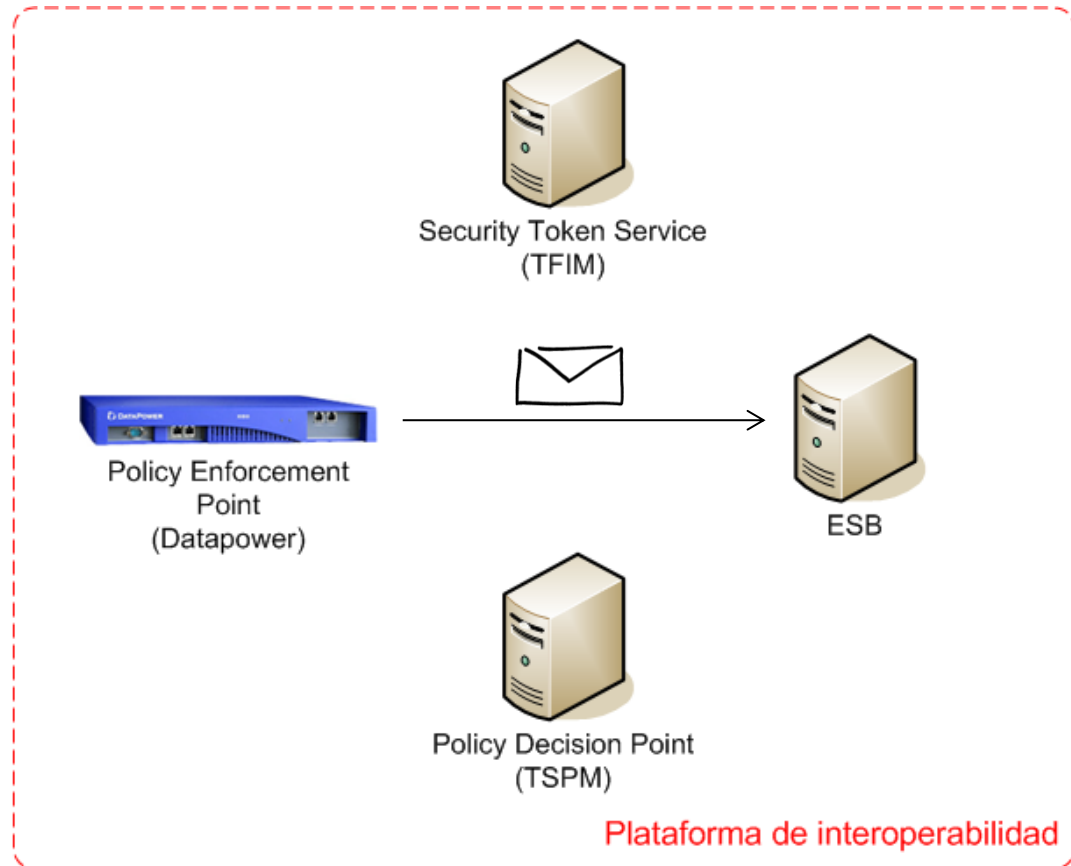
Policy Decision Point (TSPM)

Plataforma de interoperabilidad

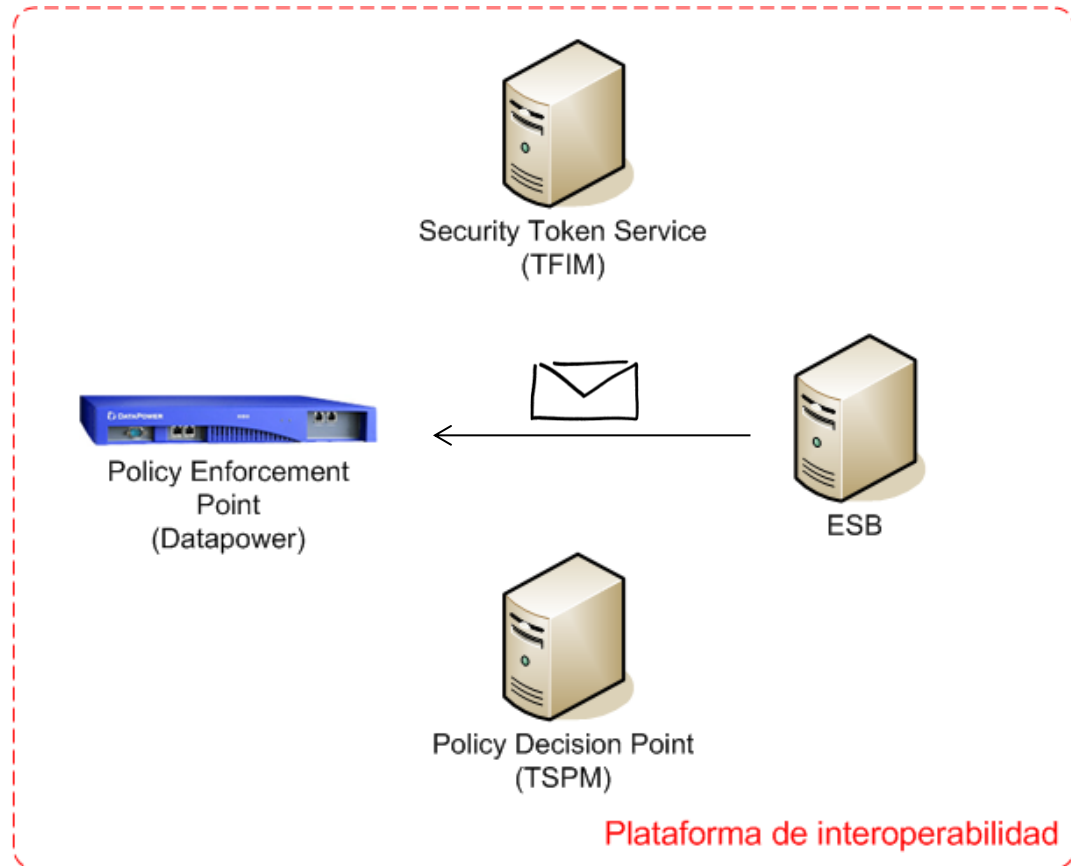
# Ruteo de mensajes en Plataforma



# Ruteo de mensajes en Plataforma

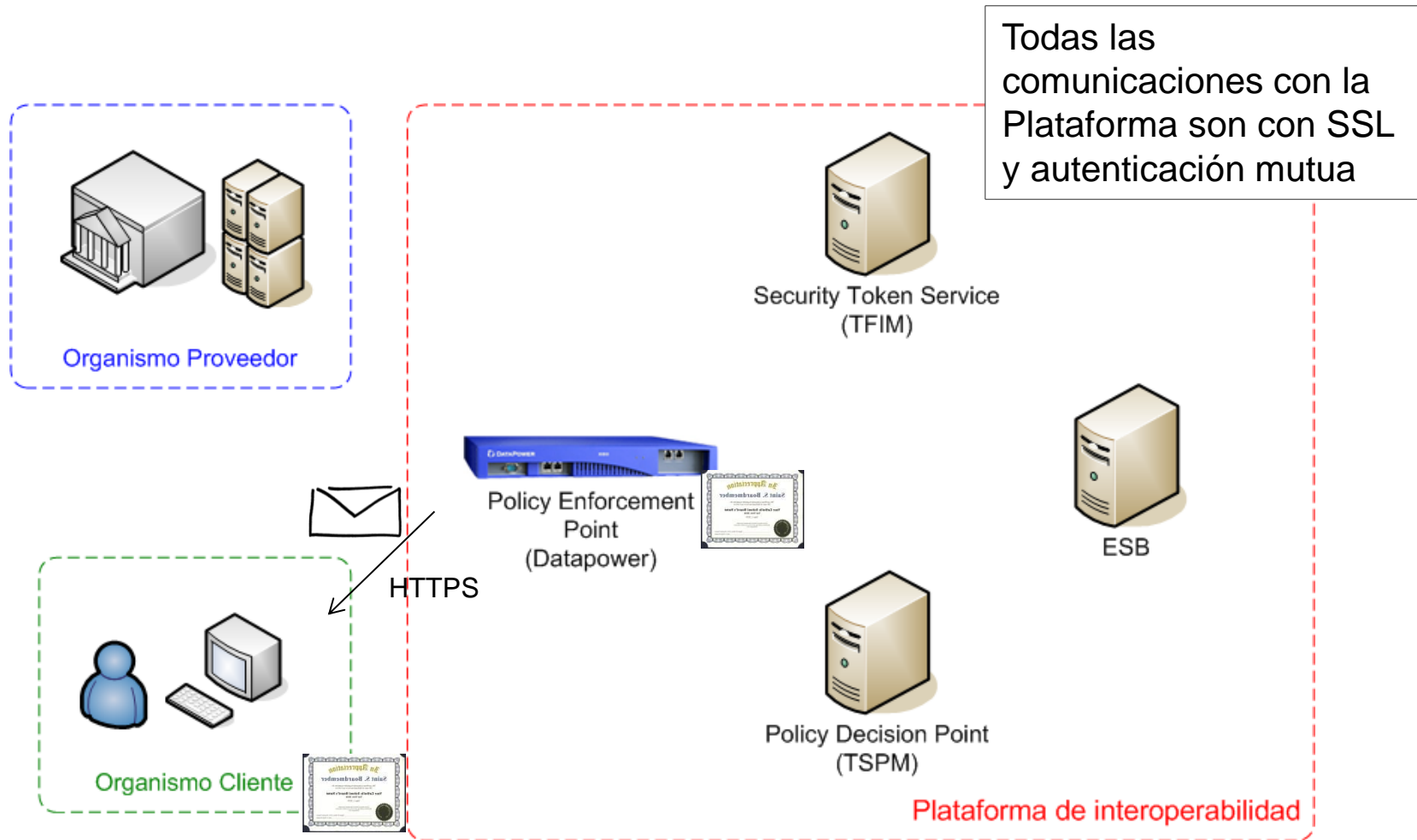


# Ruteo de mensajes en Plataforma





# Ruteo de mensajes en Plataforma



# Ejemplo Completo



## Mensaje para el STS

- Servicio a consumir
- Token SAML
  - Rol del usuario
  - Usuario
  - Firma de org.



Organismo Cliente



Security Token Service (TFIM)



Policy Enforcement Point (Datapower)



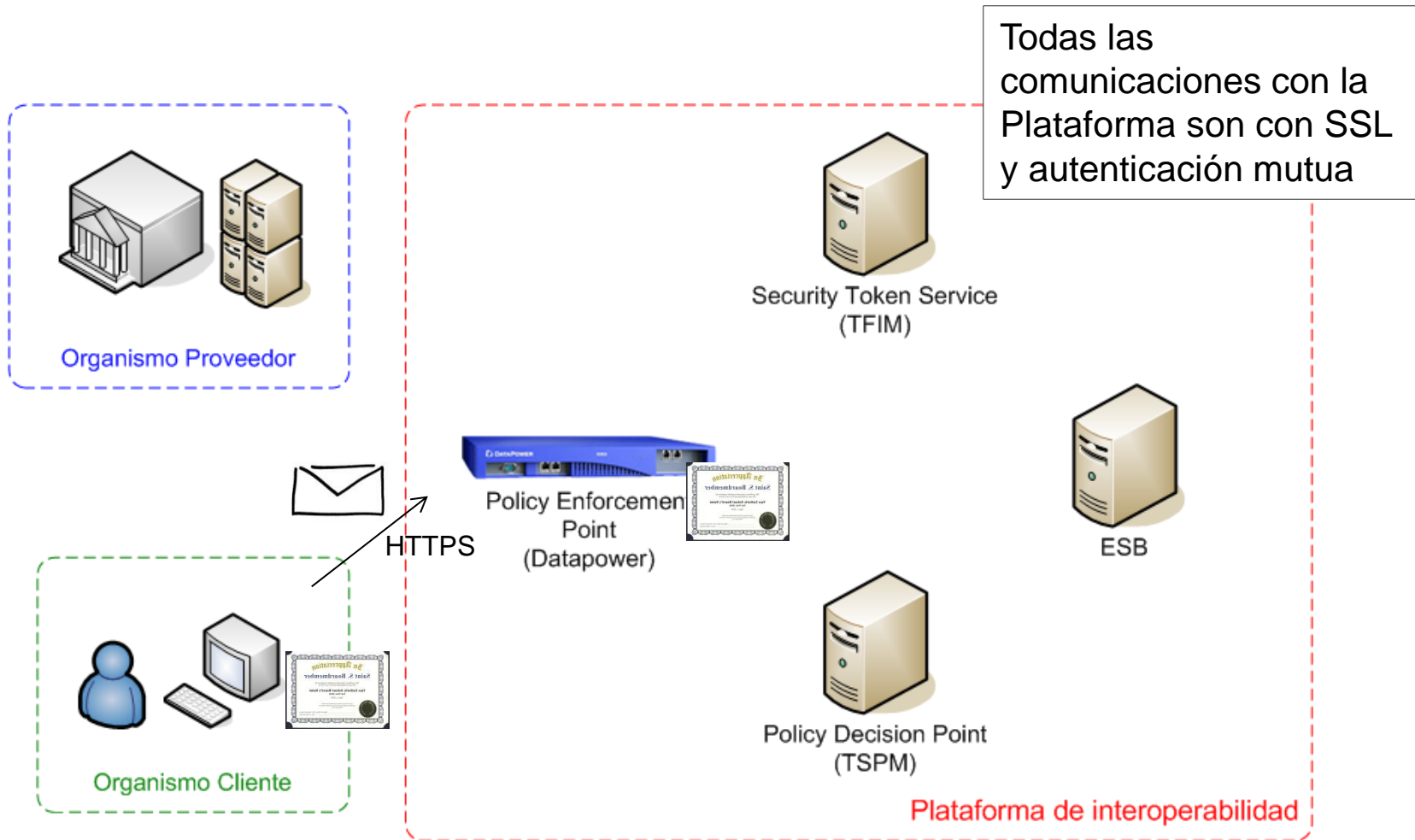
ESB



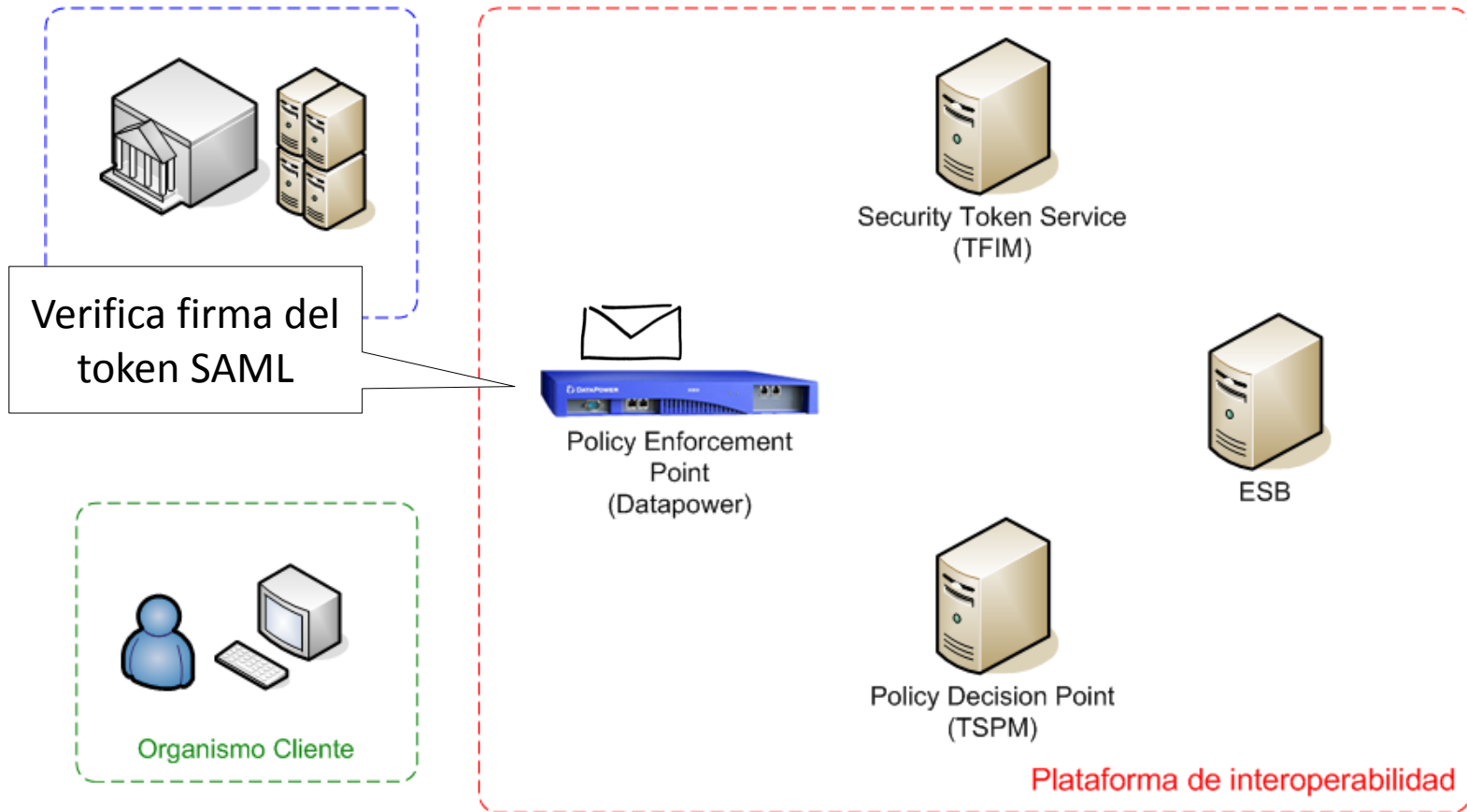
Policy Decision Point (TSPM)

Plataforma de interoperabilidad

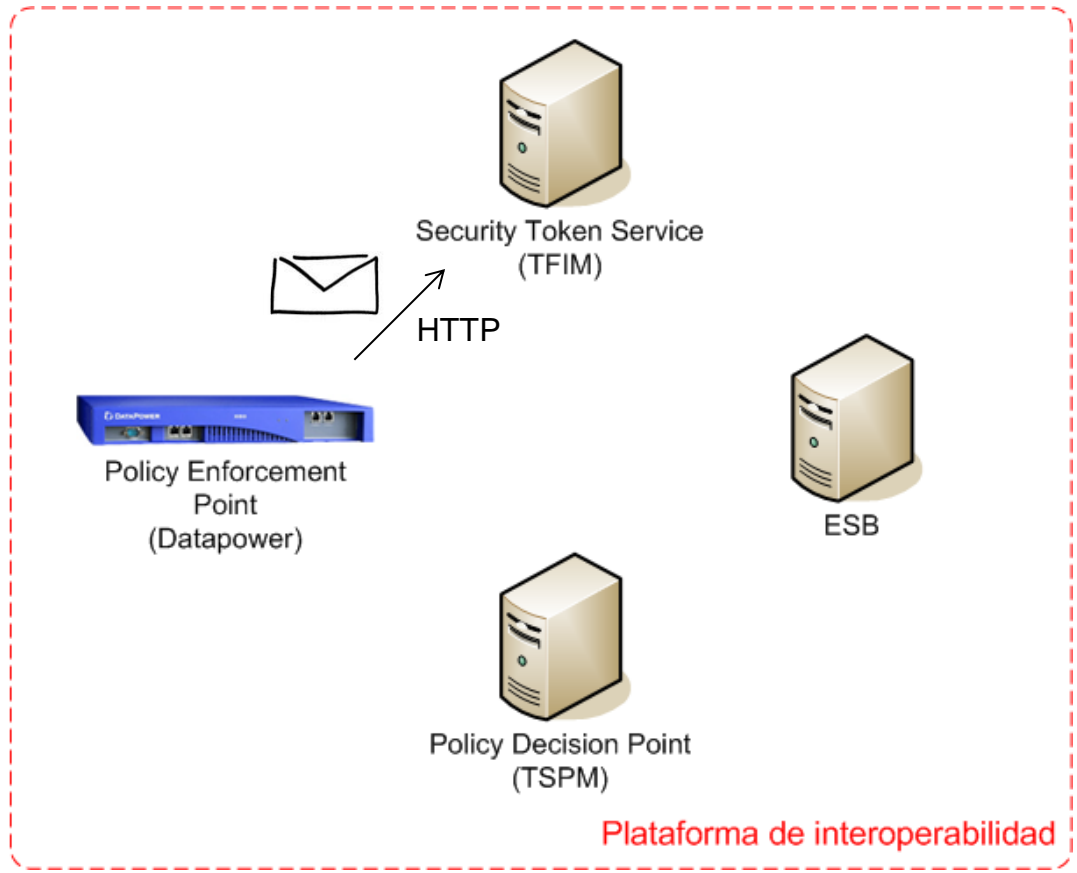
# Ejemplo Completo



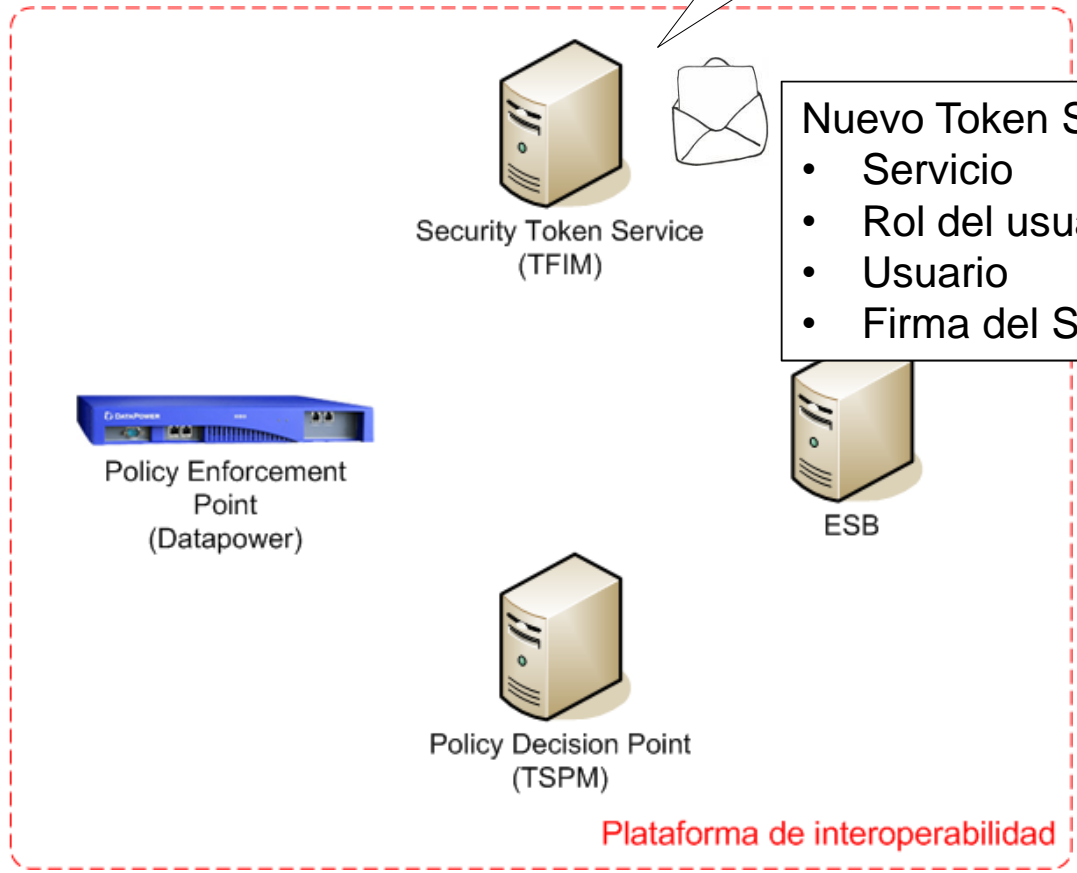
# Ejemplo Completo



# Ejemplo Completo



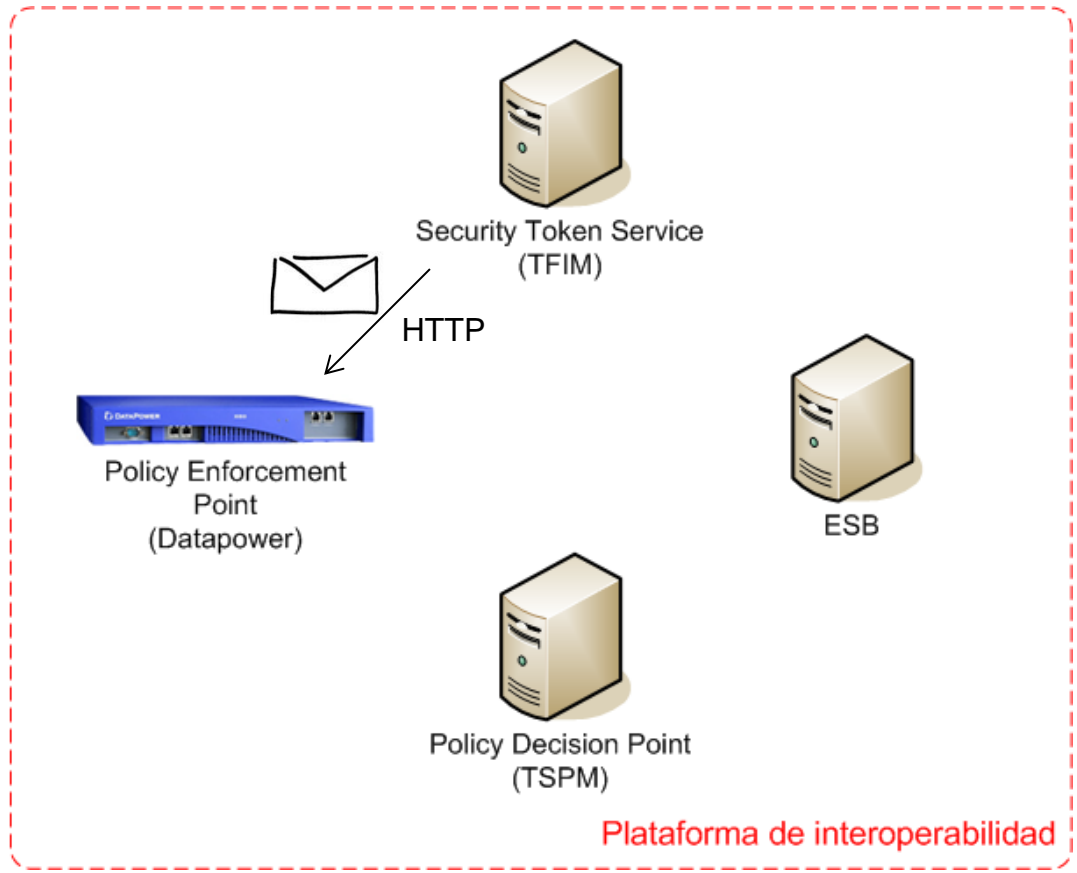
# Ejemplo Completo



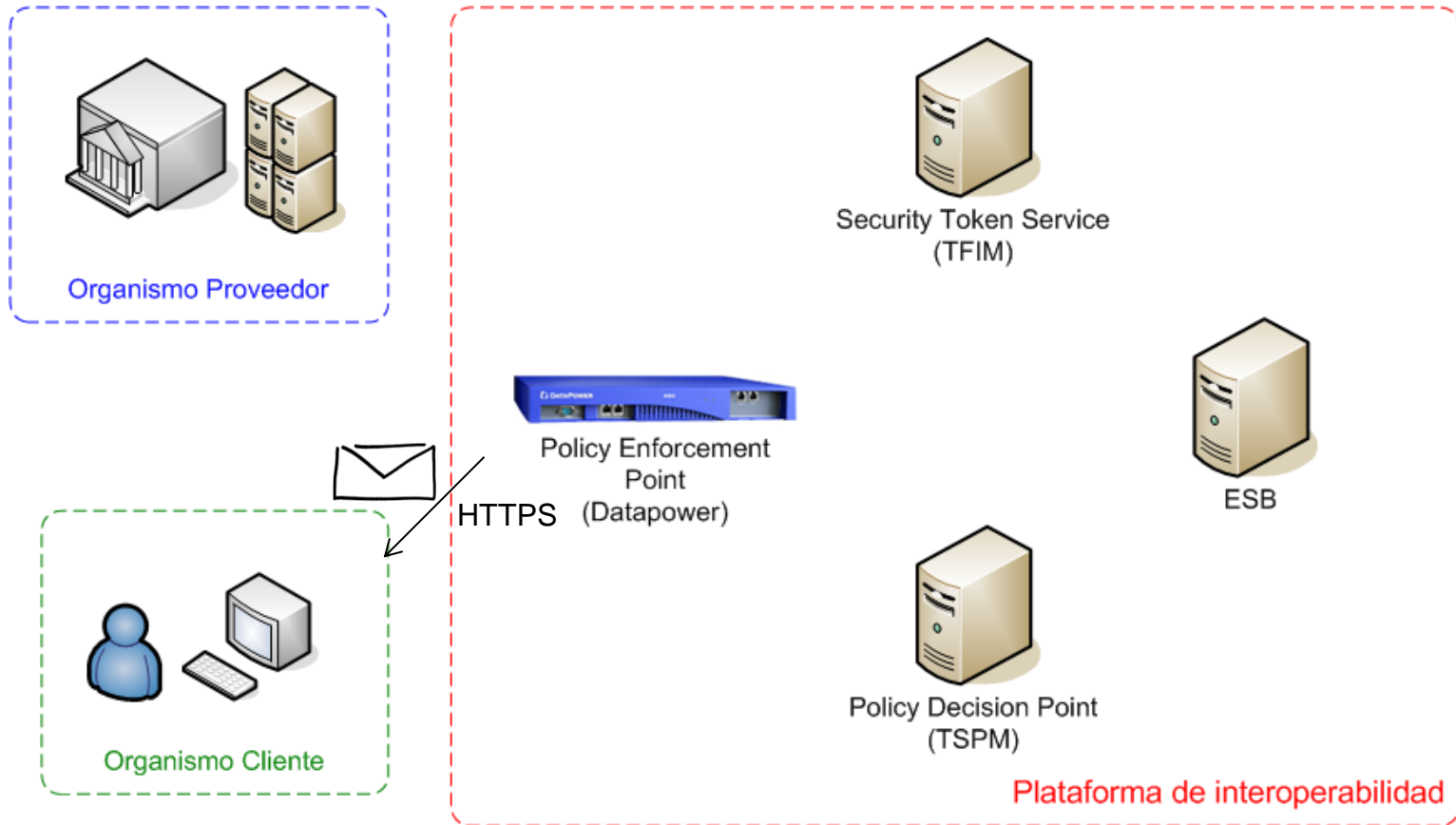
Emite nuevo token SAML

- Nuevo Token SAML
- Servicio
  - Rol del usuario
  - Usuario
  - Firma del STS

# Ejemplo Completo

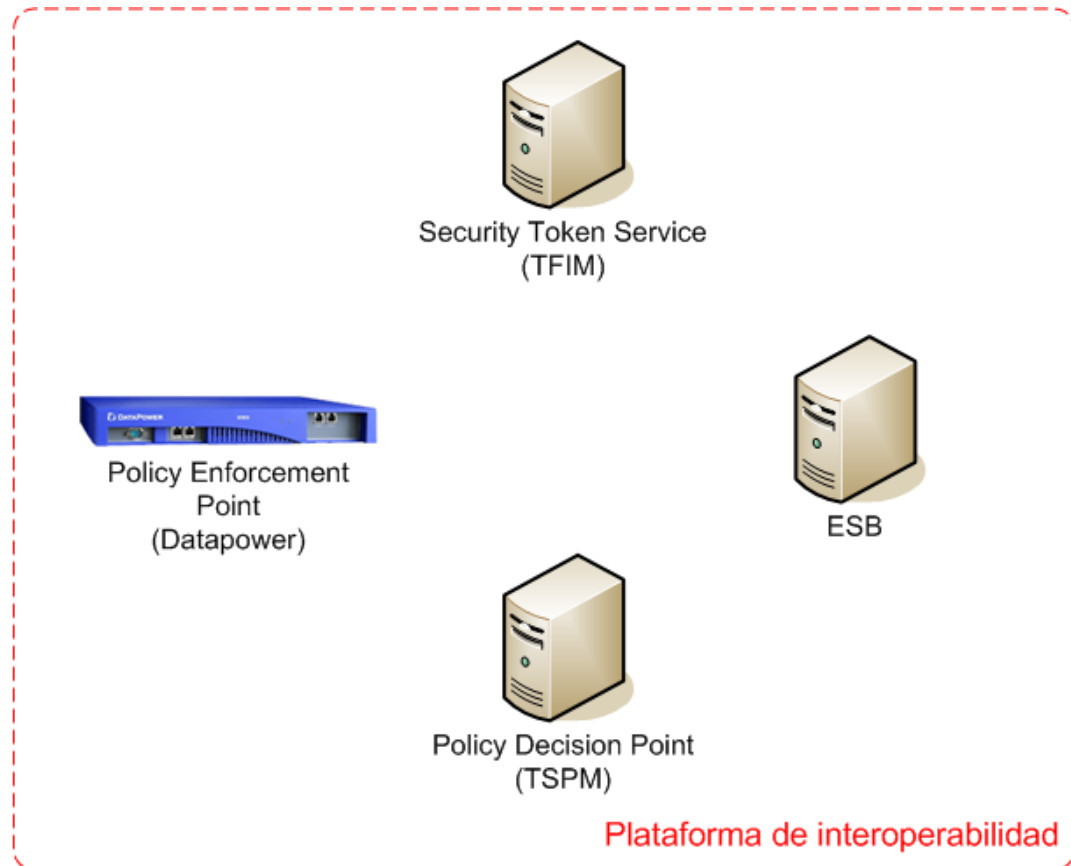
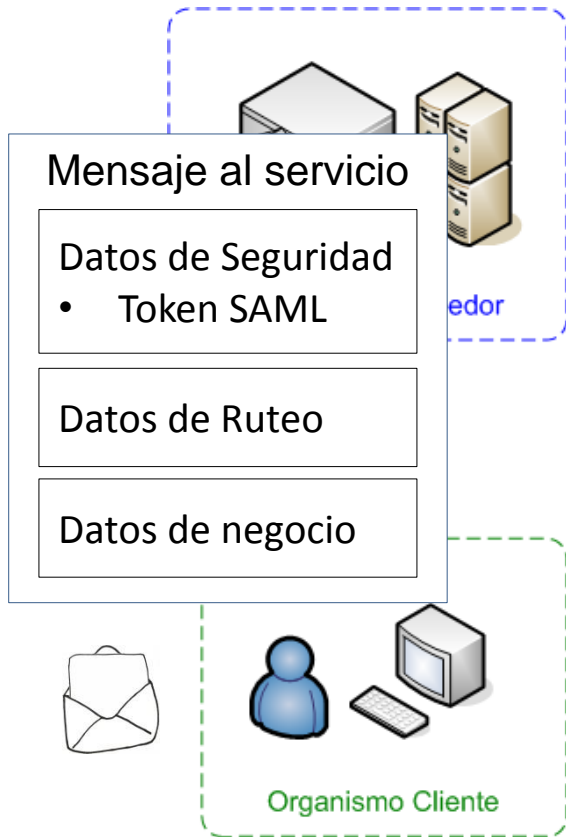


# Ejemplo Completo

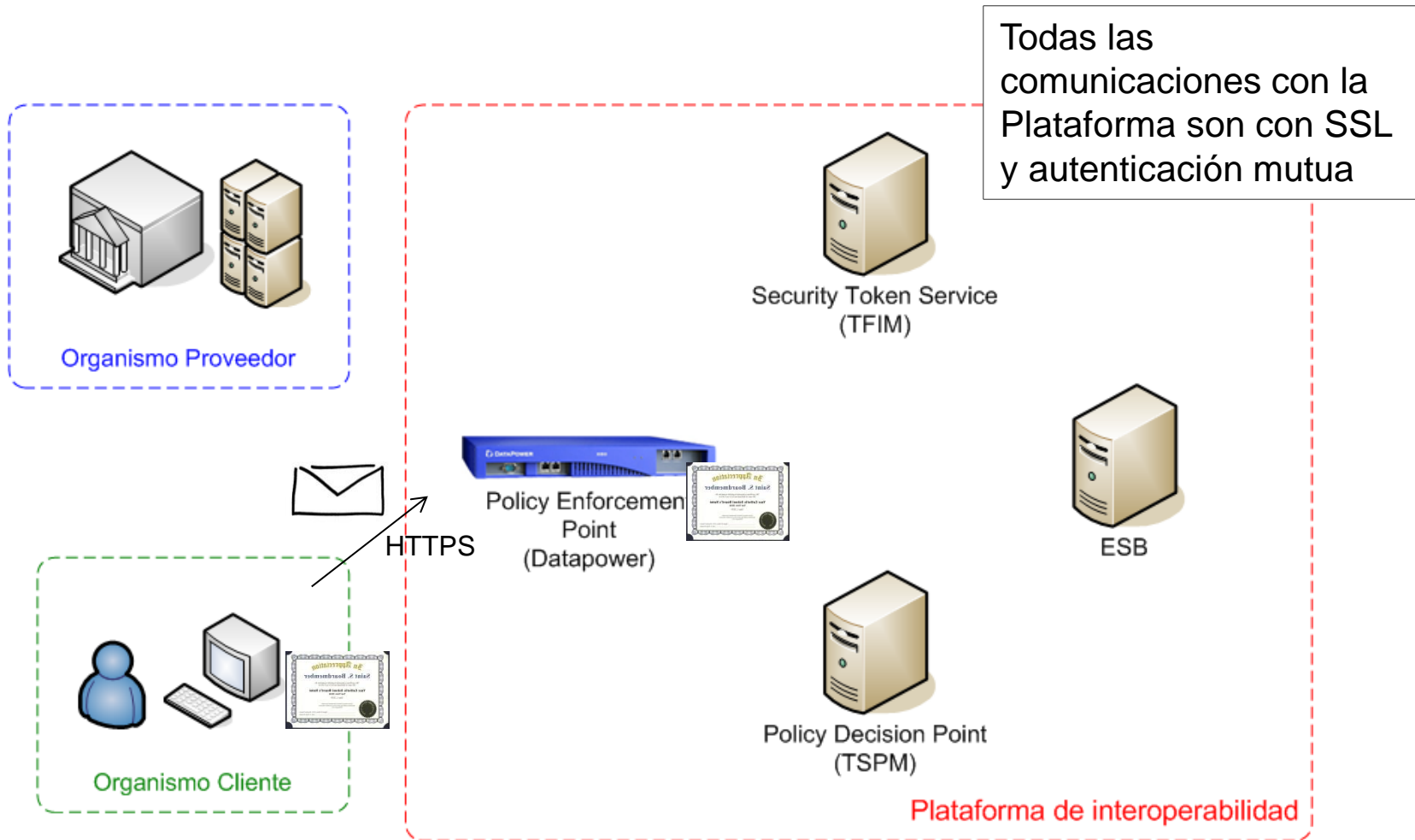




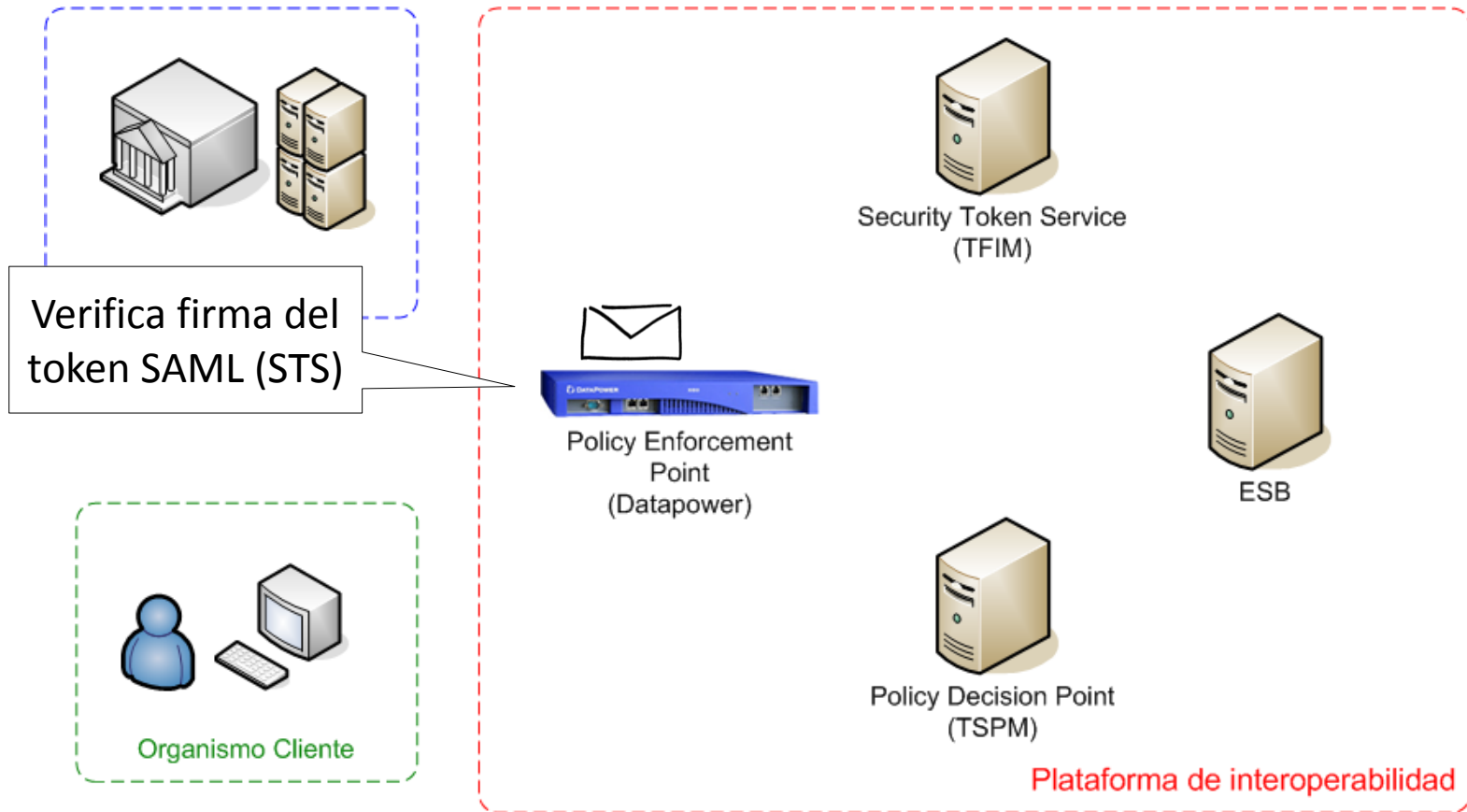
# Ejemplo Completo



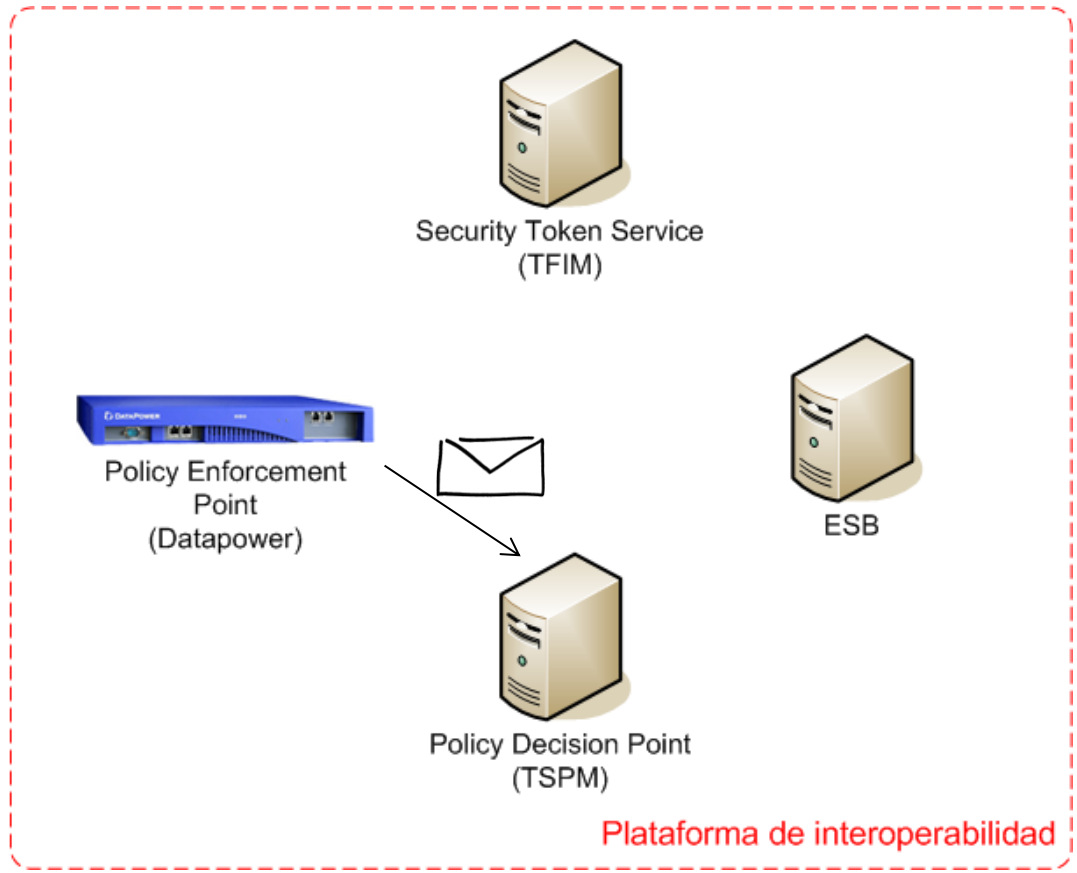
# Ejemplo Completo



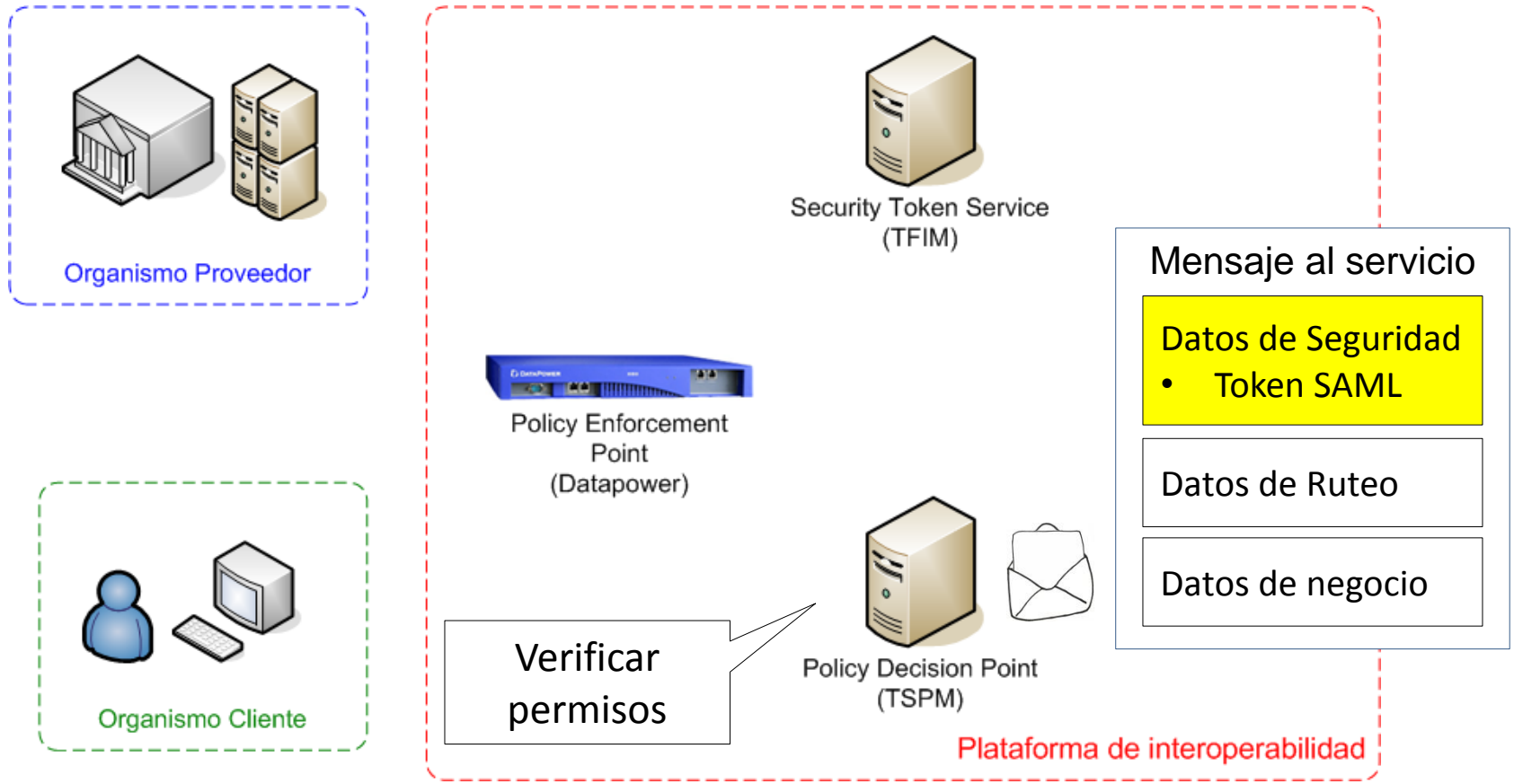
# Ejemplo Completo



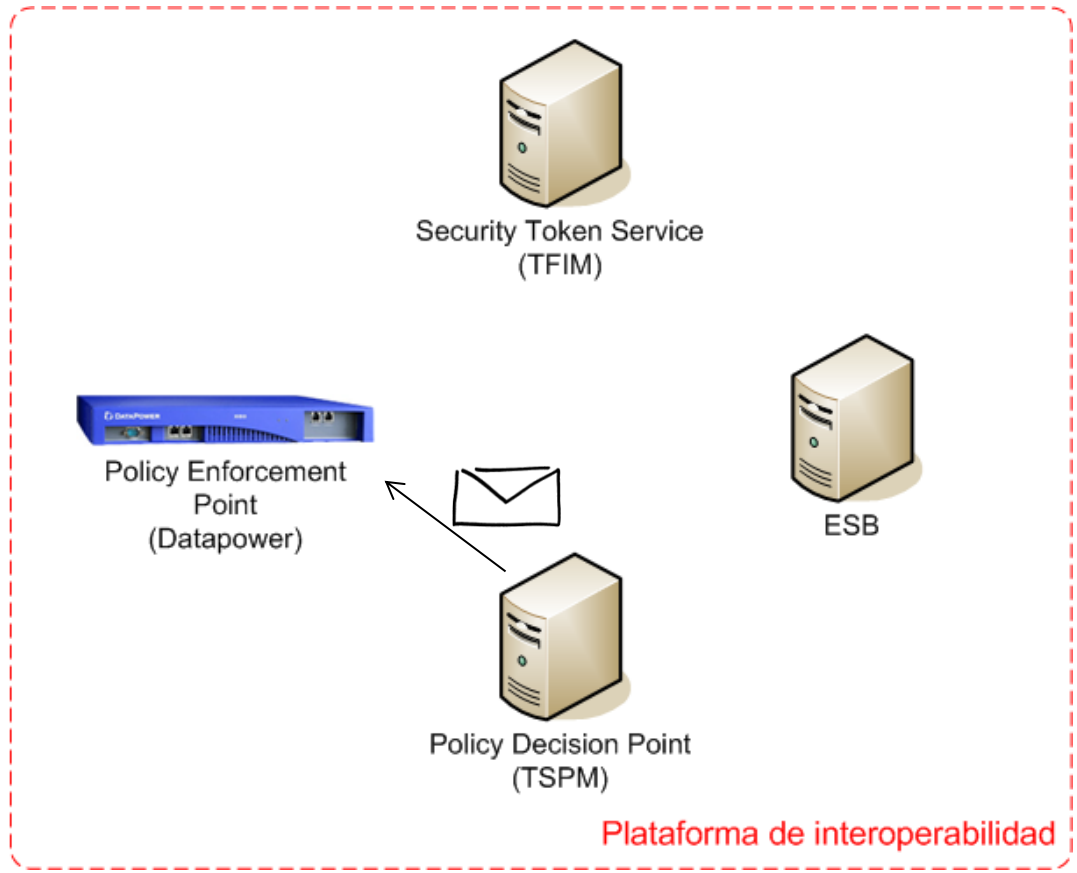
# Ejemplo Completo



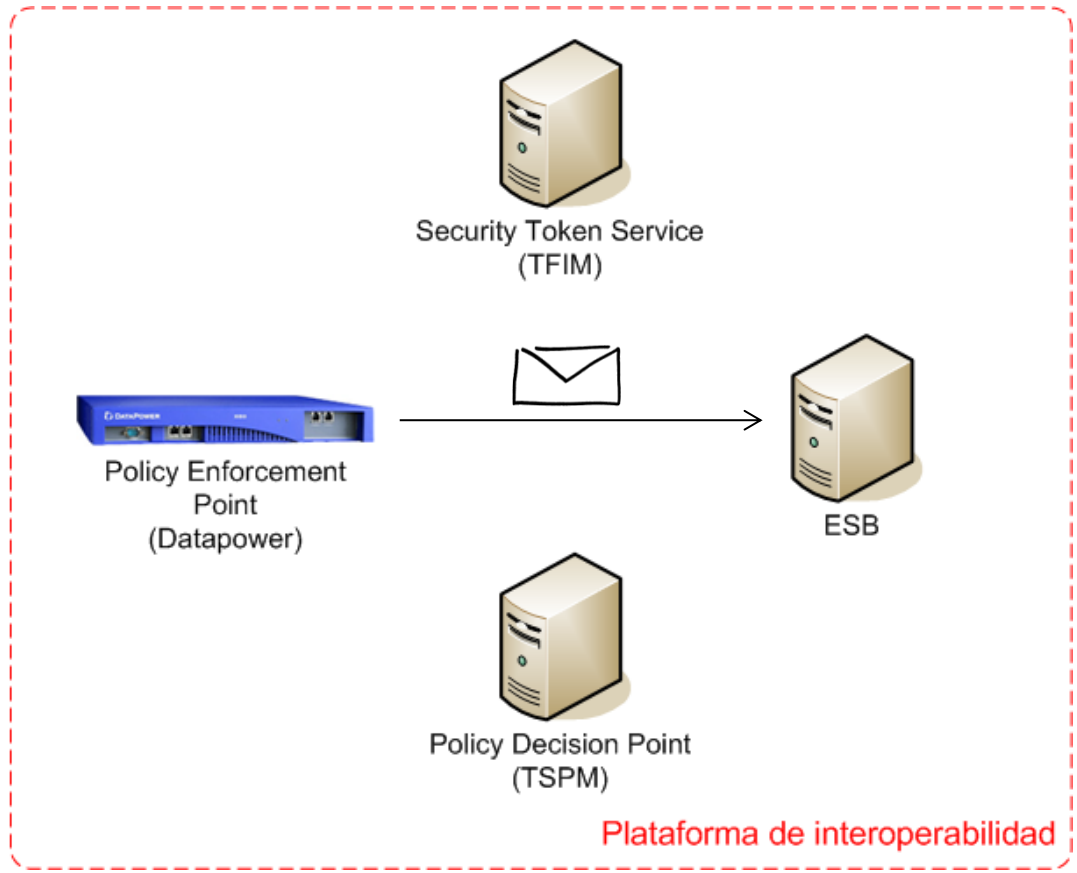
# Ejemplo Completo



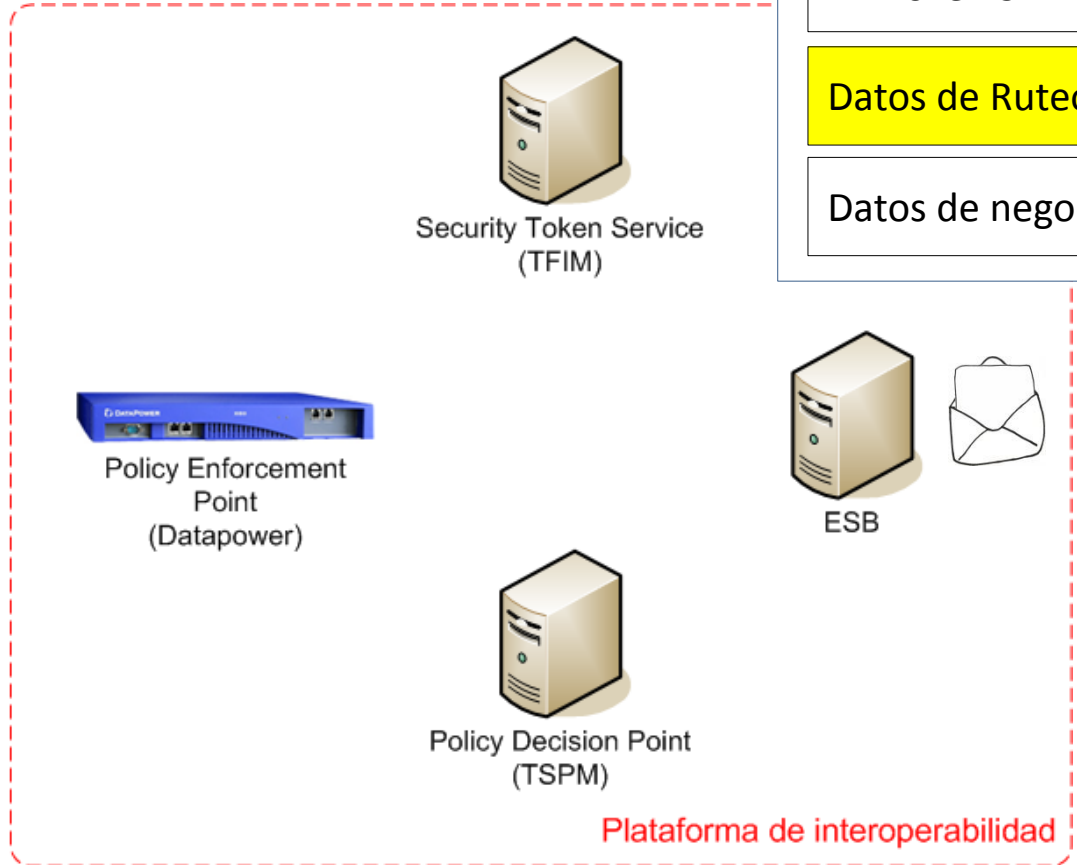
# Ejemplo Completo



# Ejemplo Completo

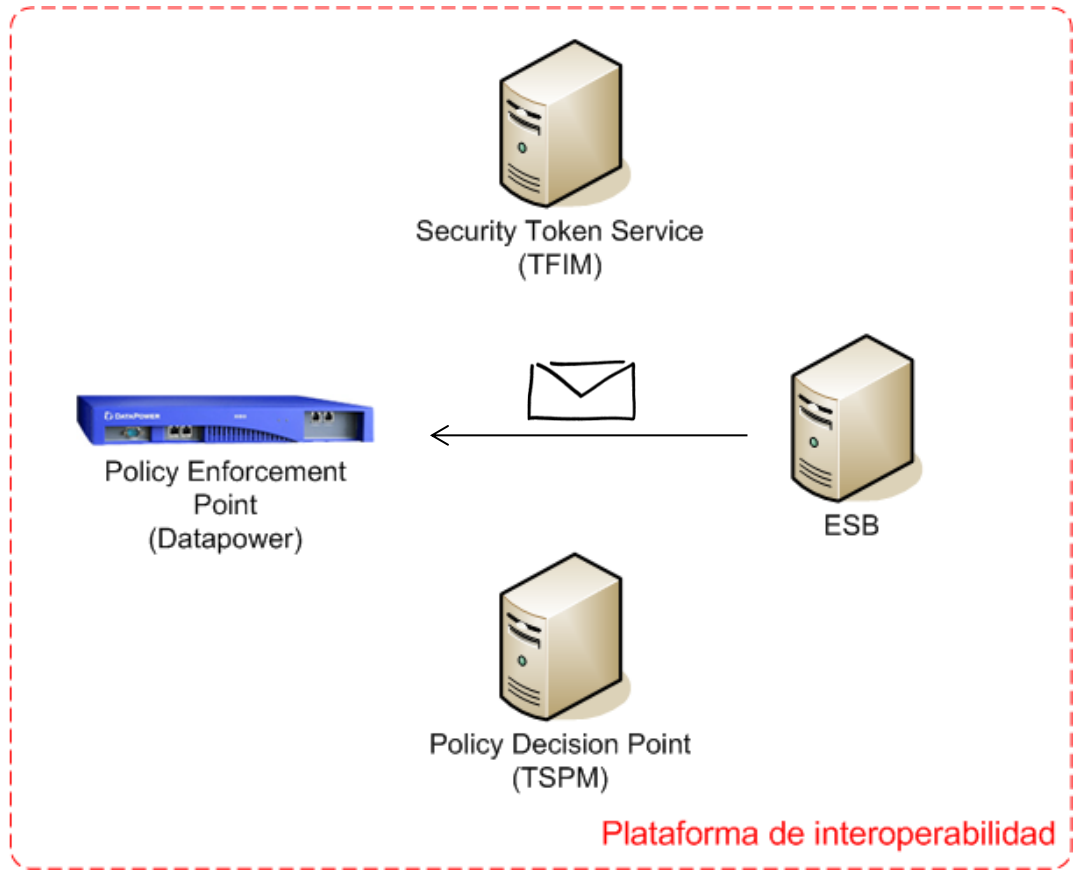


# Ejemplo Completo

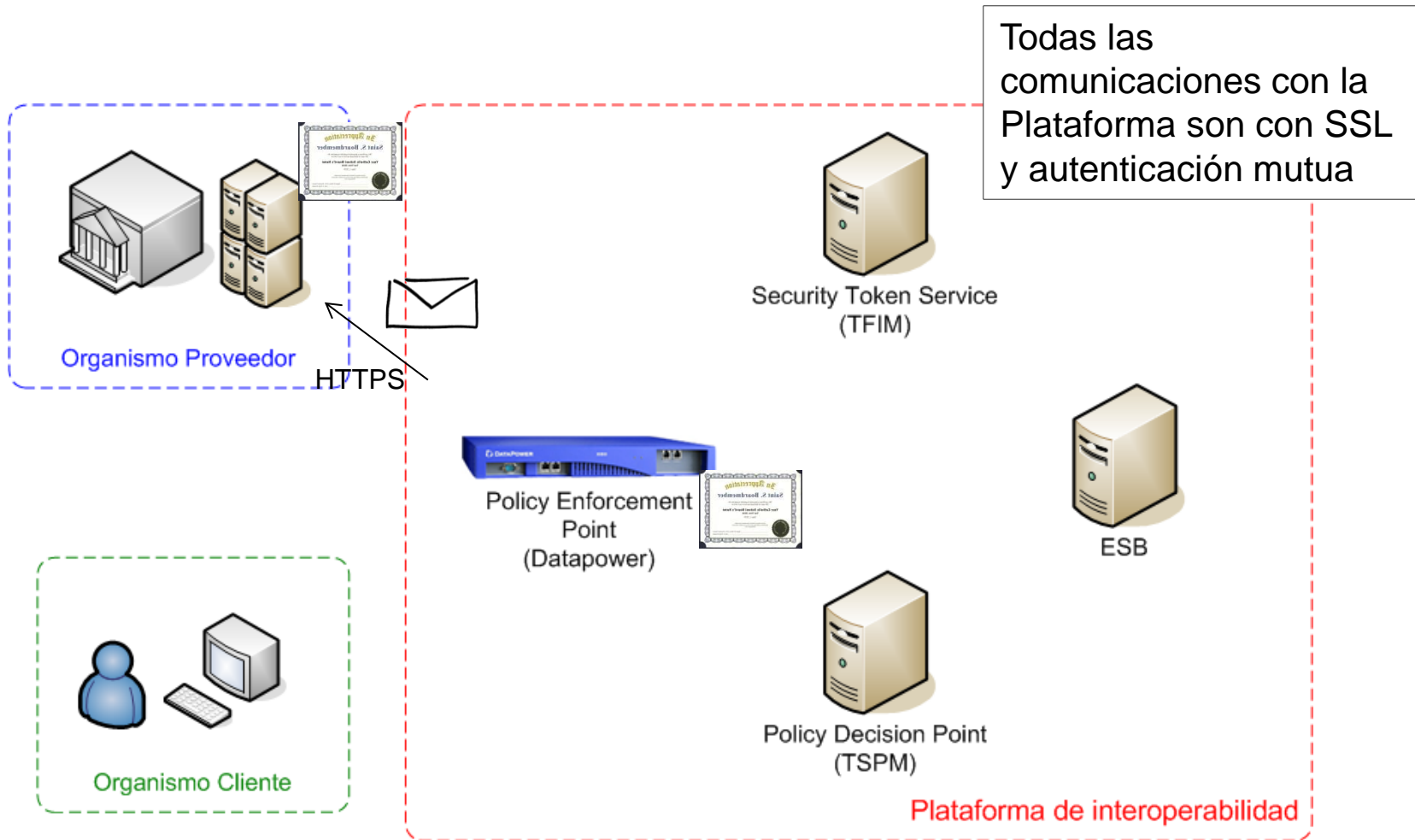




# Ejemplo Completo



# Ejemplo Completo



# Ejemplo Completo



Organismo Proveedor



Organismo Cliente



Security Token Service (TFIM)



Policy Enforcement Point (Datapower)



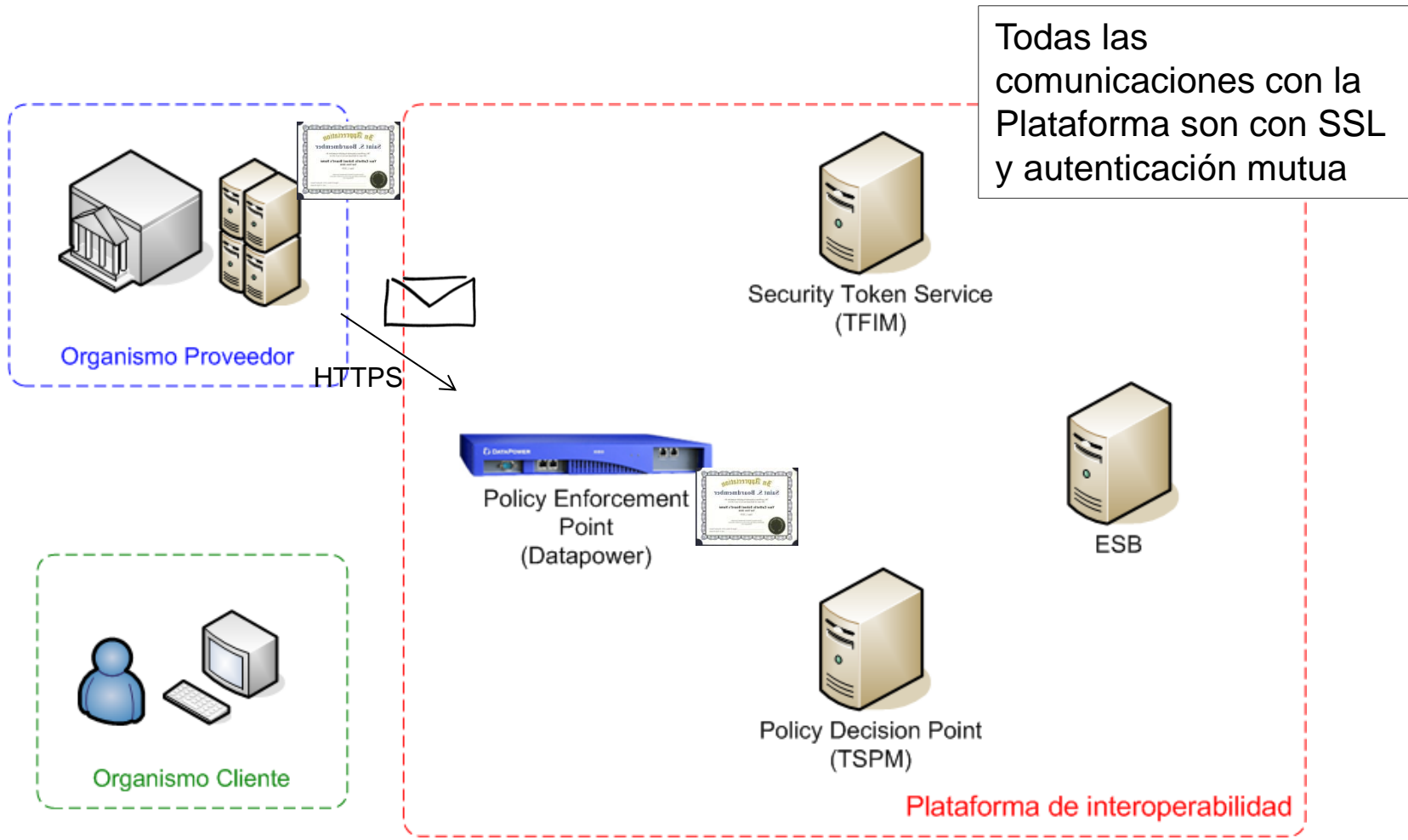
ESB



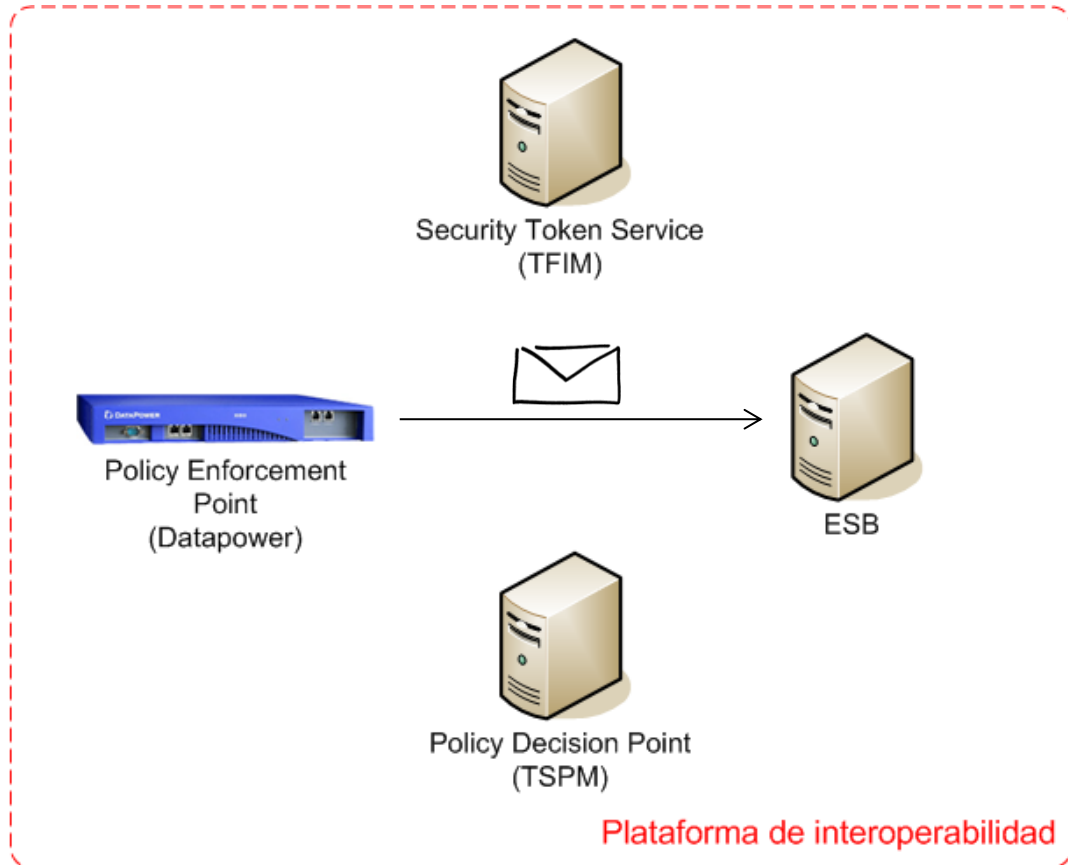
Policy Decision Point (TSPM)

Plataforma de interoperabilidad

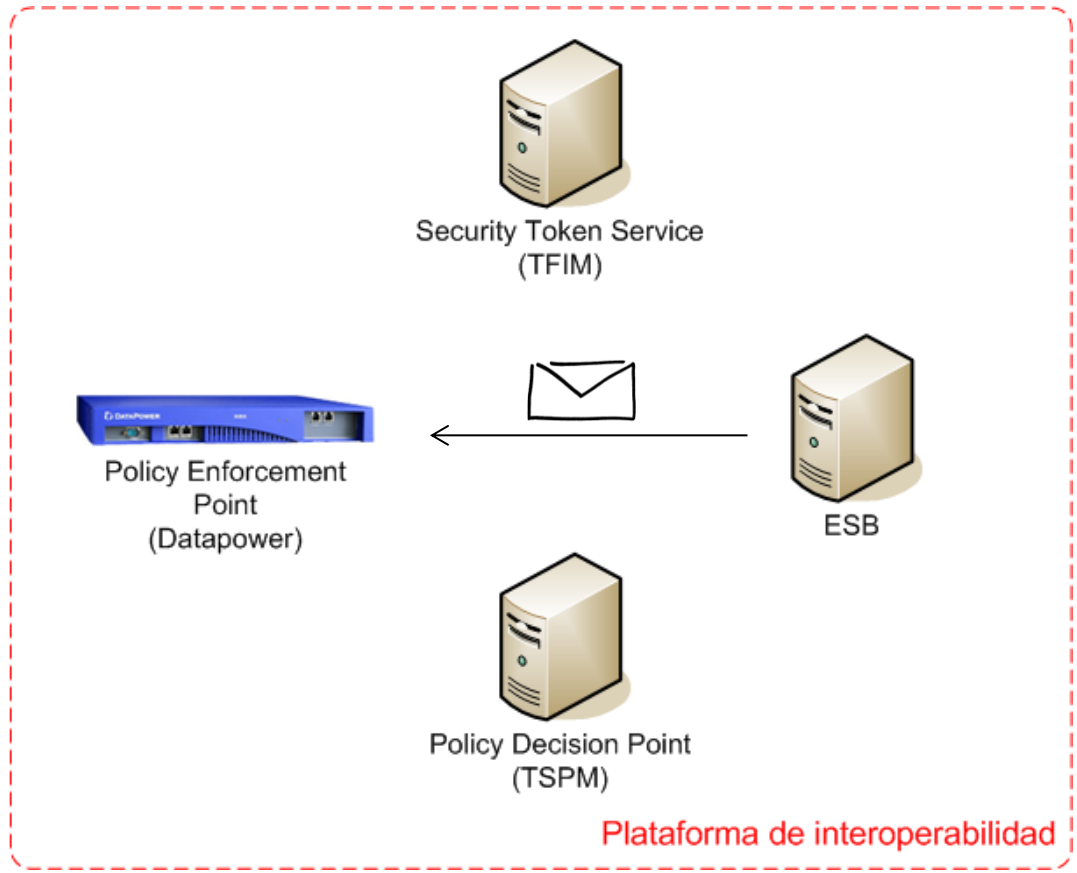
# Ejemplo Completo



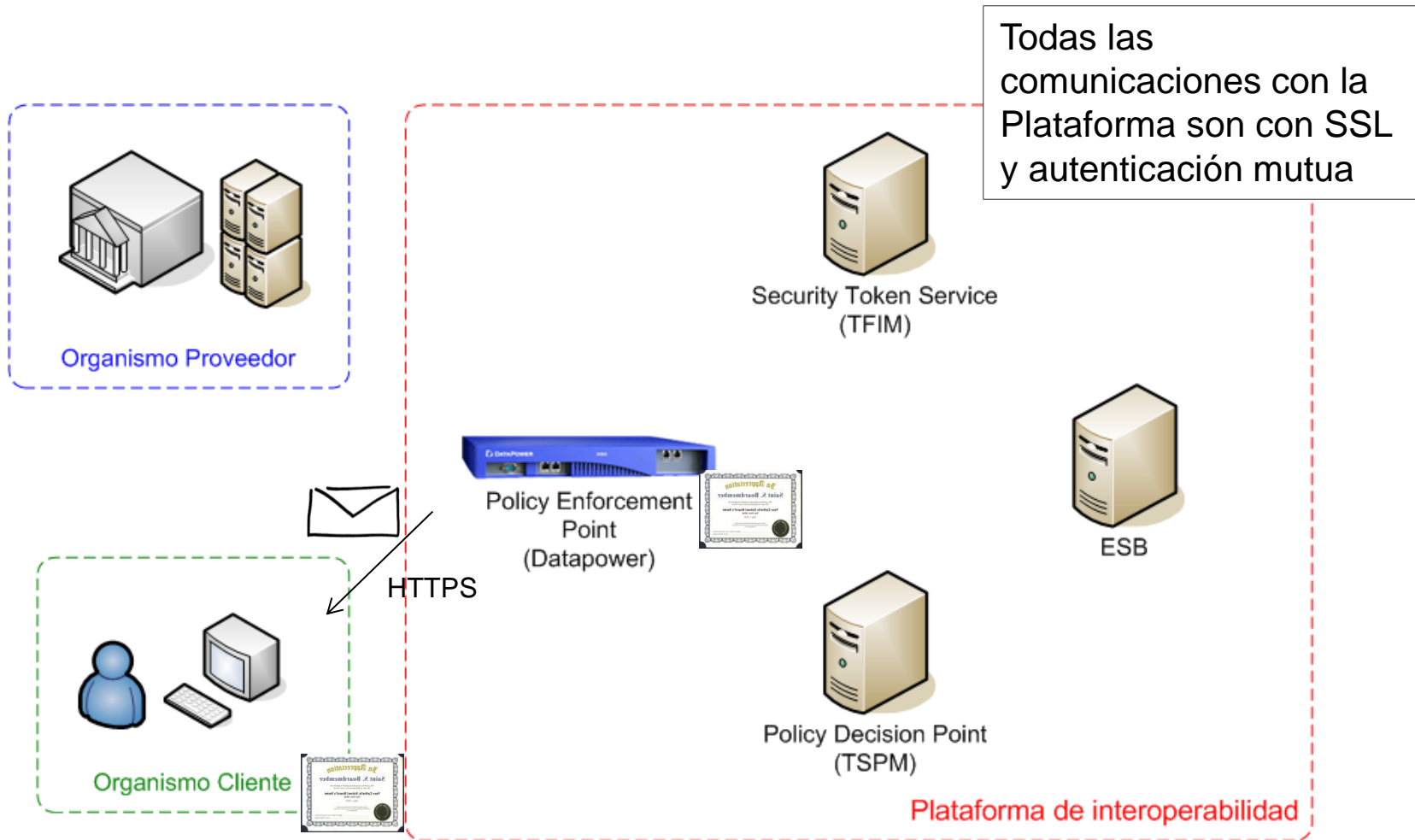
# Ejemplo Completo



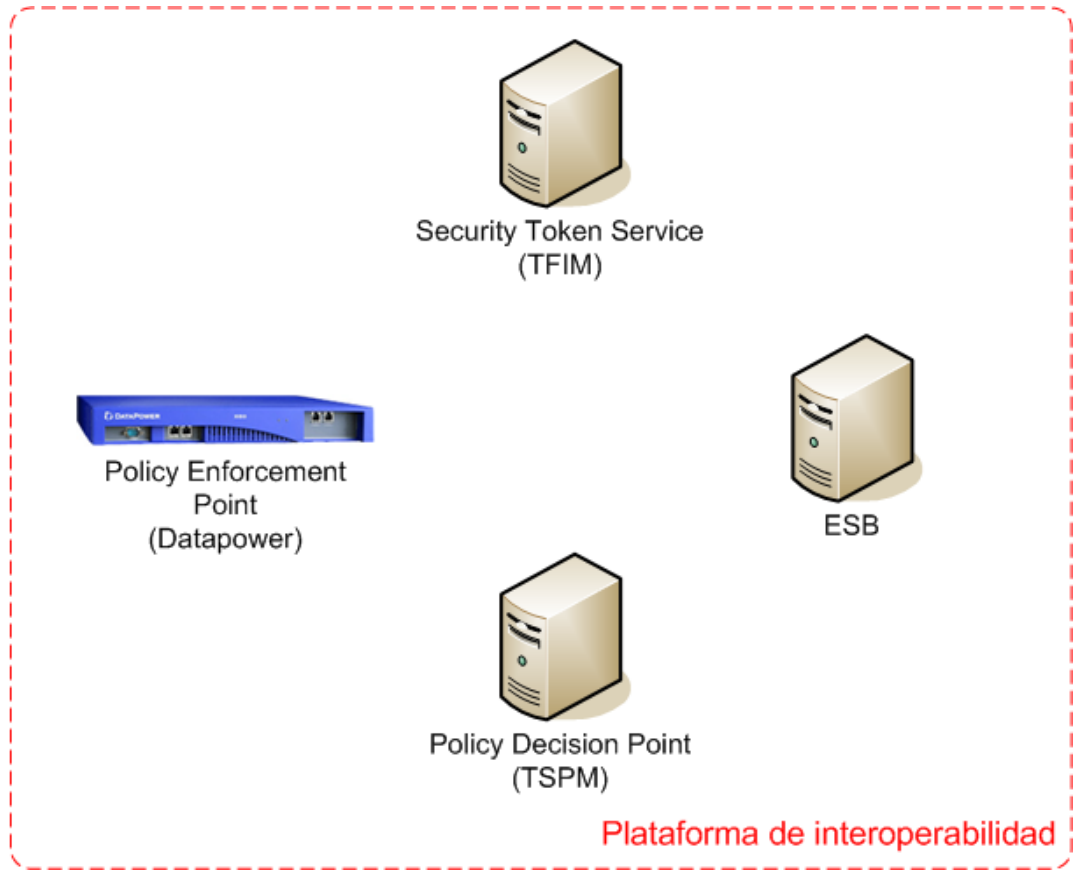
# Ejemplo Completo



# Ejemplo Completo

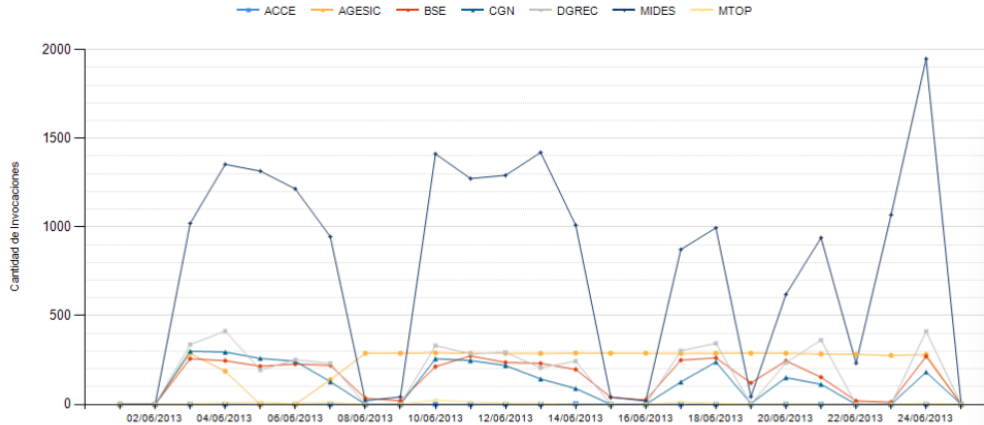


# Ejemplo Completo

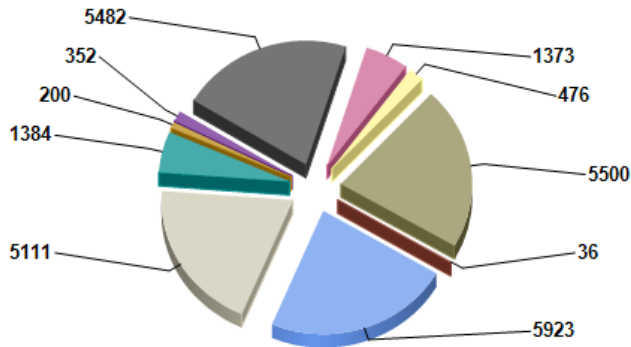




# Reportes estadísticos



Servicio Consumido	Operación Consumida	Organismo Consumidor	Fecha/Hora	Resultado	Tiempo (ms)
Servicio de Nucleos	Version - wsn	AGESIC	03/12/2012 19:40:10	Éxito	1000
Servicio de Nucleos	Env Grabar SOE Nucleo Integrante	MIDES	03/12/2012 17:20:05	Éxito	1000
Servicio de Nucleos	Env Grabar SOE Nucleo Integrante	MIDES	03/12/2012 17:20:04	Éxito	1000
Servicio de Nucleos	Env. ABM Núcleo	MIDES	03/12/2012 17:20:02	Éxito	0
Servicio de Nucleos	Obtener Col Datos Nucleo	MIDES	03/12/2012 17:20:01	Éxito	1000
Servicio de Nucleos	Env Grabar SOE Nucleo Integrante	MIDES	03/12/2012 17:17:51	Éxito	1000
Servicio de Nucleos	Env Grabar SOE Nucleo Integrante	MIDES	03/12/2012 17:17:49	Éxito	0
Servicio de Nucleos	Env. ABM Núcleo	MIDES	03/12/2012 17:17:48	Éxito	1000
Servicio de Nucleos	Obtener Col Datos Nucleo	MIDES	03/12/2012 17:17:47	Éxito	0
Servicio de Nucleos	Env. Grabar SOE Nucleo	MIDES	03/12/2012 17:16:41	Éxito	3000
Servicio de Nucleos	Env Grabar SOE Nucleo Integrante	MIDES	03/12/2012 17:16:36	Éxito	1000
Servicio de Nucleos	Env Grabar SOE Nucleo Integrante	MIDES	03/12/2012 17:16:34	Éxito	0
Servicio de Nucleos	Env Grabar SOE Nucleo Integrante	MIDES	03/12/2012 17:16:33	Éxito	1000
Servicio de Nucleos	Env. ABM Núcleo	MIDES	03/12/2012 17:16:32	Éxito	3000
Servicio de Nucleos	Obtener Col Datos Nucleo	MIDES	03/12/2012 17:16:28	Éxito	1000



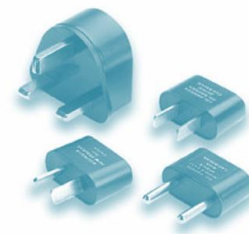
- Consultas de Certificados
- RegECA
- REMP
- Servicio CI Digital
- TimeStamp
- Datos Infantes CNVE
- RegEmpresaObra
- RUR
- Suscripcion novedades de personas
- Verificar Actividad

# Formas de consumir un servicio



- Bibliotecas Java y .NET
  - Bibliotecas desarrolladas por Agesic para simplificar el desarrollo de clientes
    - JDK 5 o 6 y JBoss 5 o 6
    - .NET 3.0 o superior
- Conector PGE
  - Software tipo caja negra que simplifica aún más el desarrollo!
  - Basado en JBoss ESB

# Conector PGE



## Intercambio **Seguro**

- WS-Trust
- WS-Security
- SSL

## Marco legal y técnico

- SAML
- Firma digital
- Certificados

## Diseño **SOA**

- Web Services
- WS-Addressing

**Es necesario...** pero **requiere de madurez en TI**

# Conector PGE

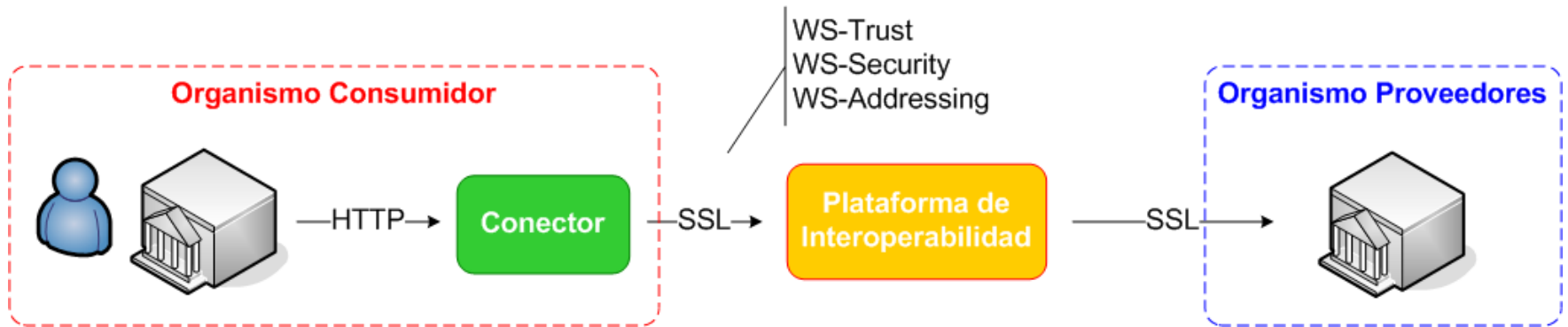


Conexión **Simple**

## Comunicaciones seguras y estándares

**Administrado** por los Organismos

**Open** Source



# Mesa de Servicios



## Servicio

Horario de atención: lunes a viernes de 9 a 18hs

Contacto: telefónico o vía e-mail [soporte@agesic.gub.uy](mailto:soporte@agesic.gub.uy)

Tiempo de respuesta: 1 hora

## Ventajas

Contacto recibido ante un incidente consumado

Se proporciona información de diagnóstico

Acelera resolución de incidentes

Agiliza contacto con otras áreas de AGESIC

# Conclusiones

## Utilizar el Catálogo

- Buscar el servicio que deseo consumir
- Leer cuidadosamente la información

## Correo a Mesa de Servicios

- Correo: [soporte@agesic.gub.uy](mailto:soporte@agesic.gub.uy)
- Mencionar Servicio y Marco del Consumo

## Completar Formulario

- MDS Responde con un Formulario
- Completarlo y responder el correo

# Conclusiones

- Se presentó la plataforma de interoperabilidad y sus principales componentes
- Se describió cómo es el mecanismo de consumo de servicios
- Se presentó un escenario de ejemplo

# ¿Preguntas?







**Muchas gracias!**