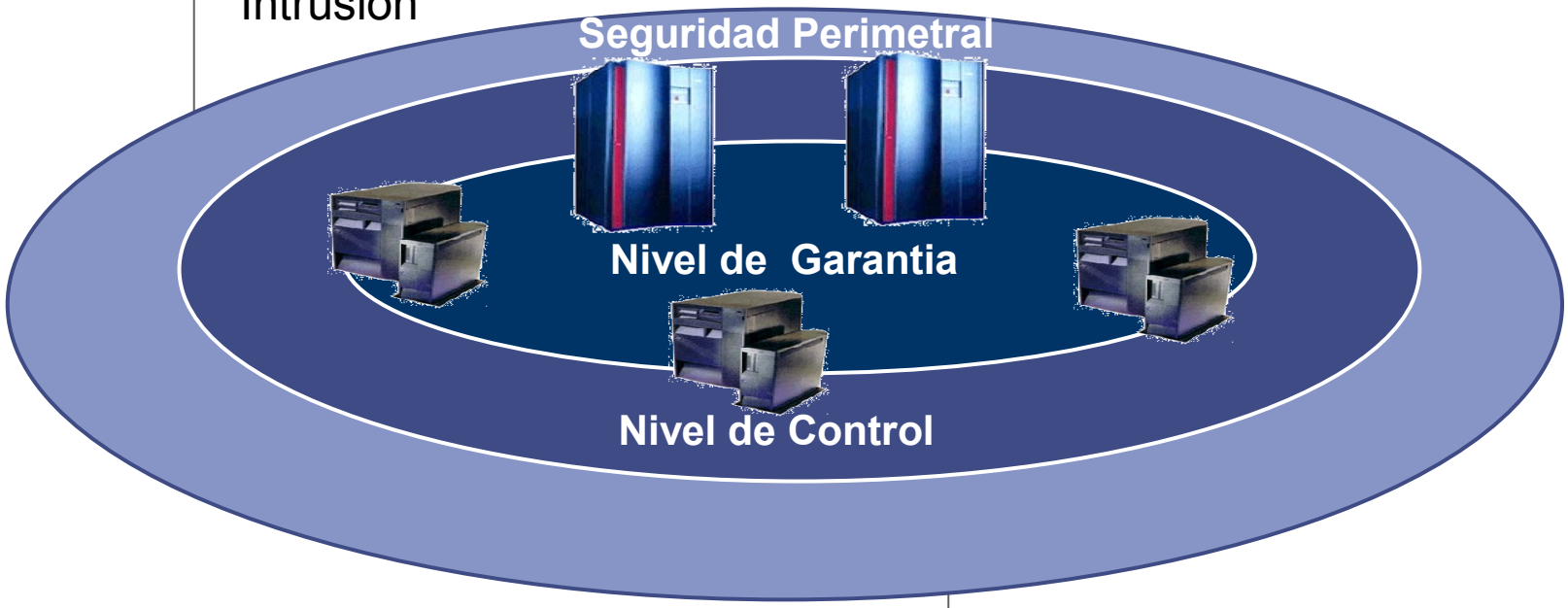
Tivoli Integrated Identity Management Software

Soluciones de IBM para la Seguridad Informática

Juan Nemiña Gantes
Tivoli Security IT Consultant

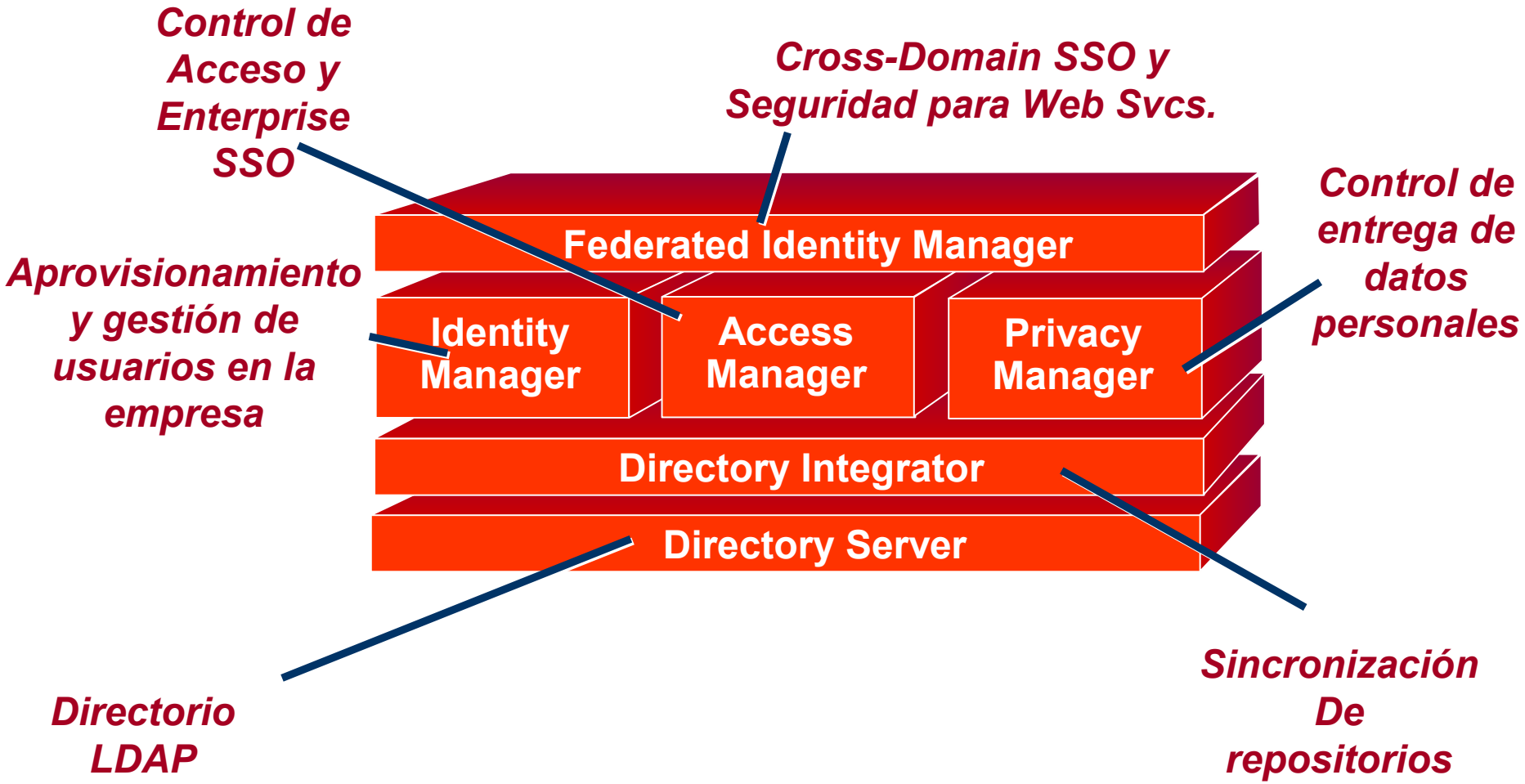
Situando el contexto: En que aspecto de la seguridad se focaliza IBM?

Muchos productos de seguridad están orientados a la seguridad perimetral: Firewalls, VPN, Anti-Virus, Detectores de Intrusion



…IBM se dedica a controlar a los que ya están dentro y a garantizar que se “comportan adecuadamente”

Catálogo Integrado de IBM para la gestión de identidades



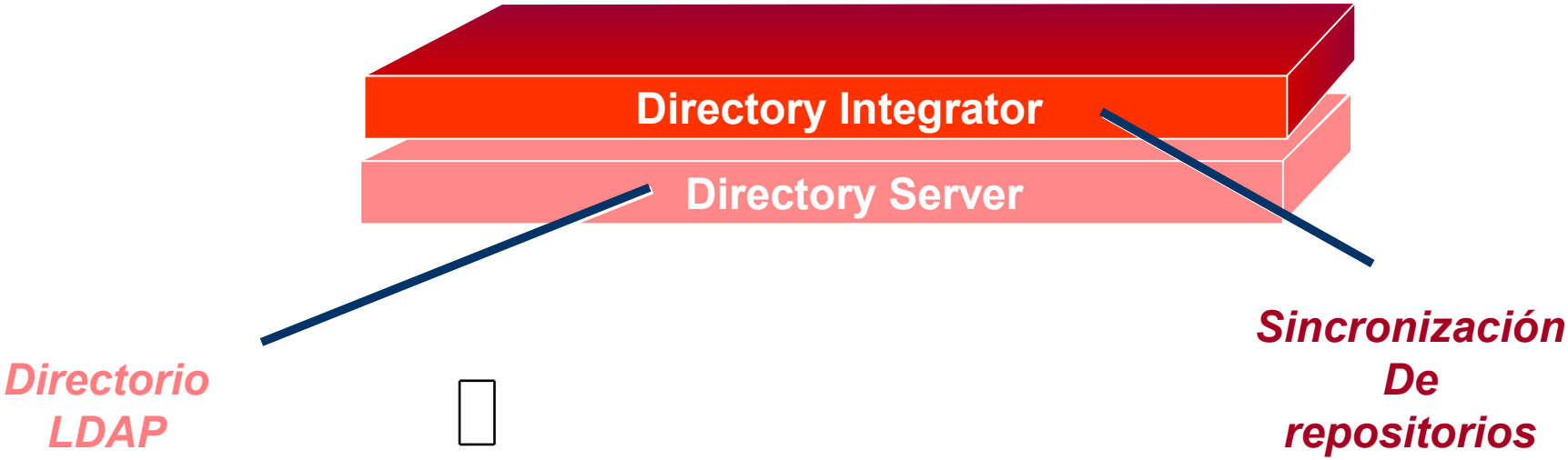
ITDS – IBM Tivoli Directory Server

- Disponible en mas sistemas operativos que ningún otro del mercado
- Construido sobre la base de datos mas rápida del mercado: IBM DB2 UDB v8.1. Muy rápido y escalable
- Completamente standard : Open Group – LDAP Certified Directory Server

Directorio LDAP

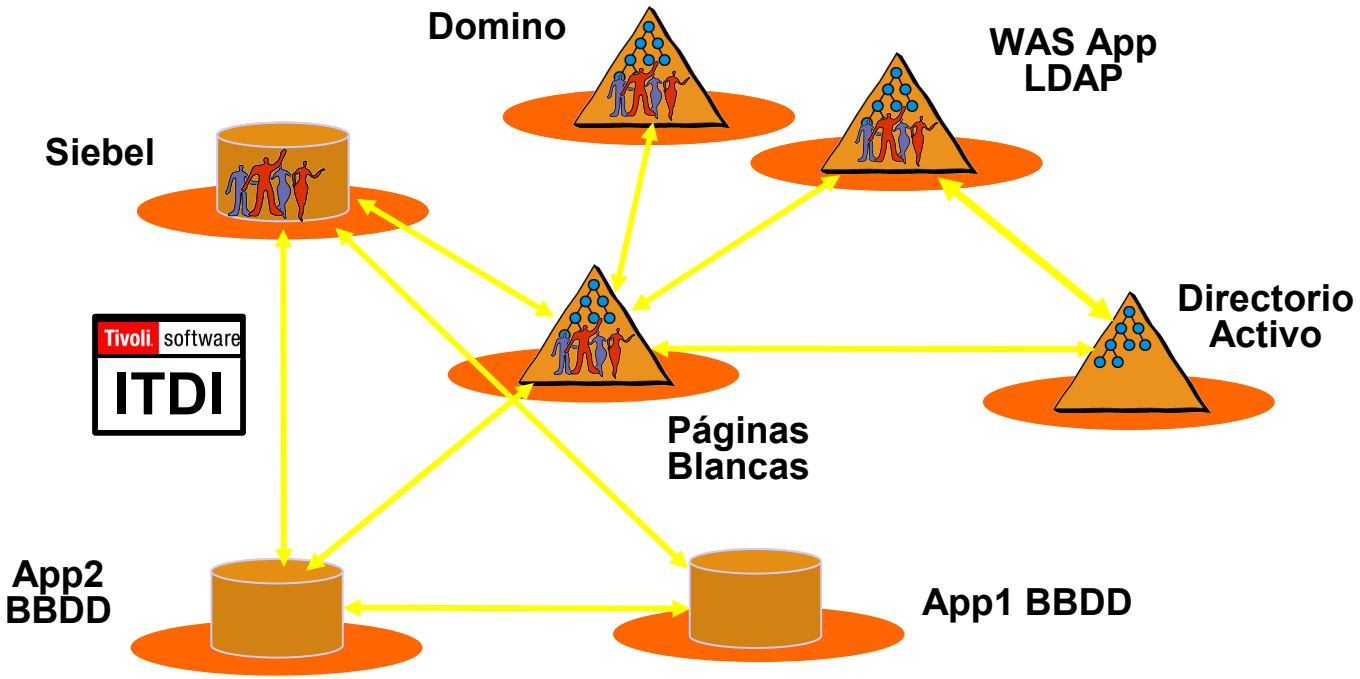
ITDI – IBM Tivoli Directory Integrator

Un entorno de integración de datos de propósito general, en tiempo real y comandado por eventos.



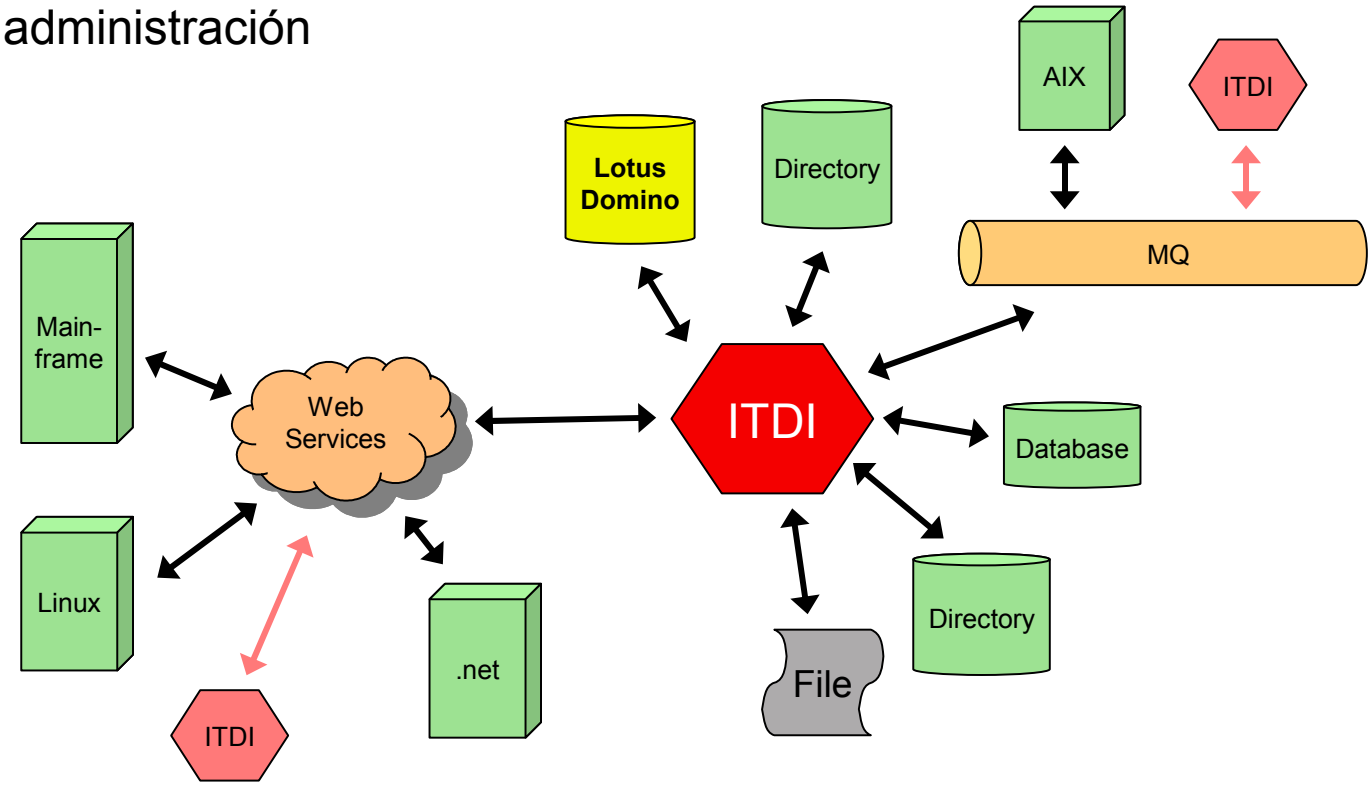
Problemática objetivo: Sincronización de directorios

- Propagación de altas, bajas y modificaciones de cuentas de usuario entre directorios
- Cualquier escenario en que se necesite propagar datos entre repositorios heterogeneos



IBM Tivoli Directory Integrator: Componentes

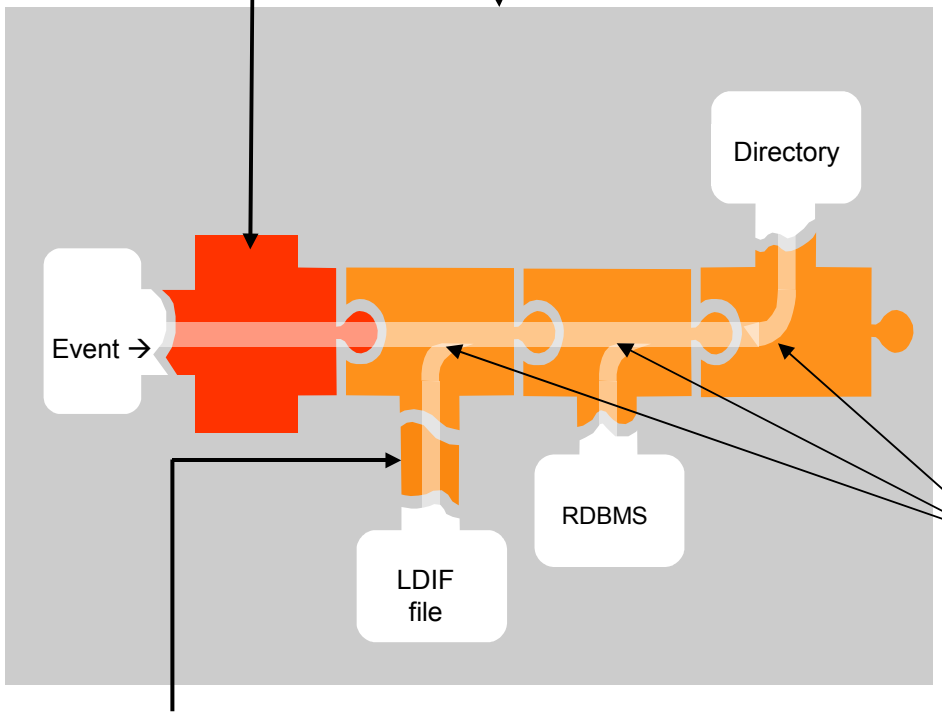
- Una GUI de desarrollo rápido, para la construcción y mantenimiento de las reglas de transformación, transporte y sincronización de datos
- Un servidor multi-threaded que ejecuta reglas y monitoriza eventos
- Una consola de administración



IBM Tivoli Directory Integrator: Elementos Lógicos

EventHandler

El paradigma evento-condición-acción permite al sistema responder a eventos predefinidos, en tiempo real



AssemblyLine

Conjunto de elementos que implementa el flujo de integración, basado en la configuración de sus componentes individuales: conectores, parsers, etc y la llógica que conduce el proceso

Connector

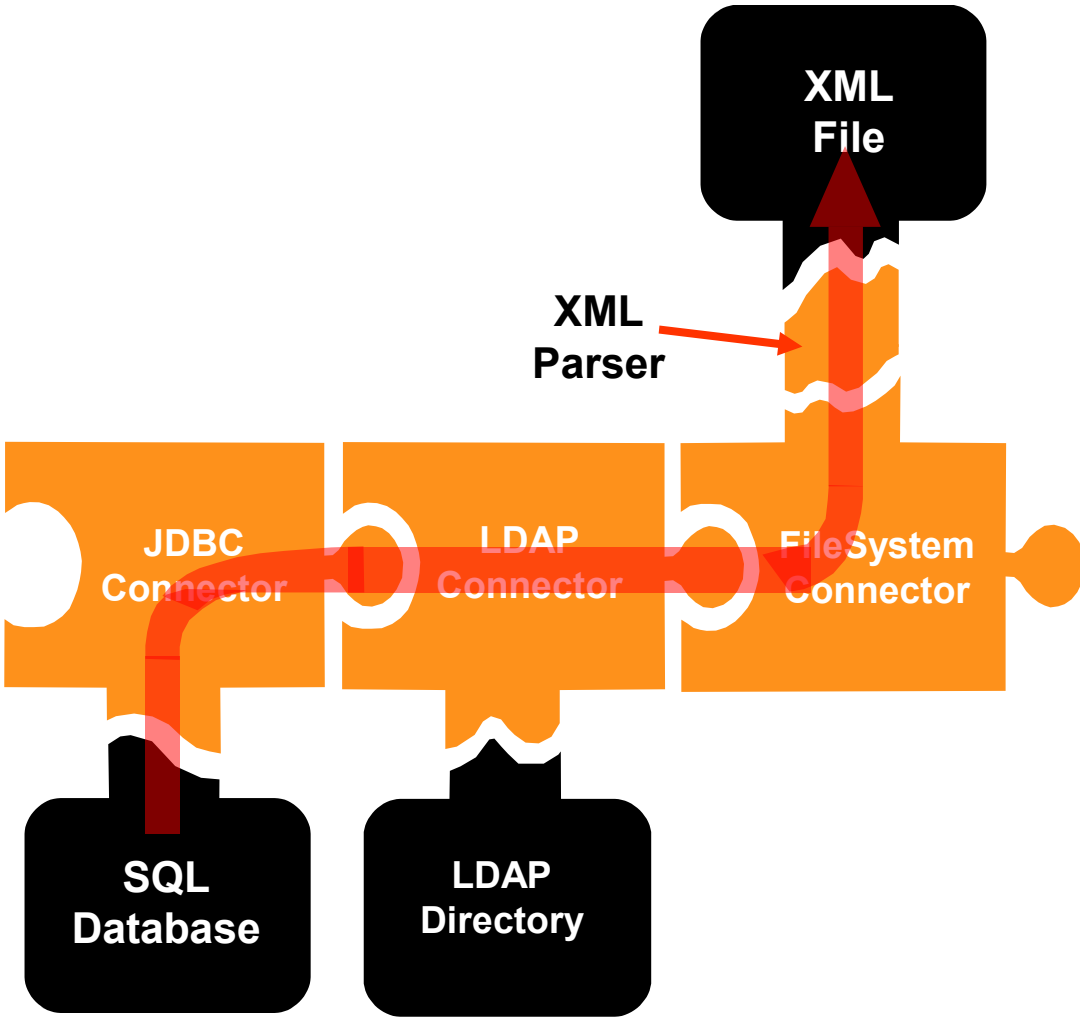
Conecta con el dispositivo, aplicación, BBDD o sistema pertinente y realiza la acción requerida: búsqueda, iteración, borrado, modificación, etc

Parser

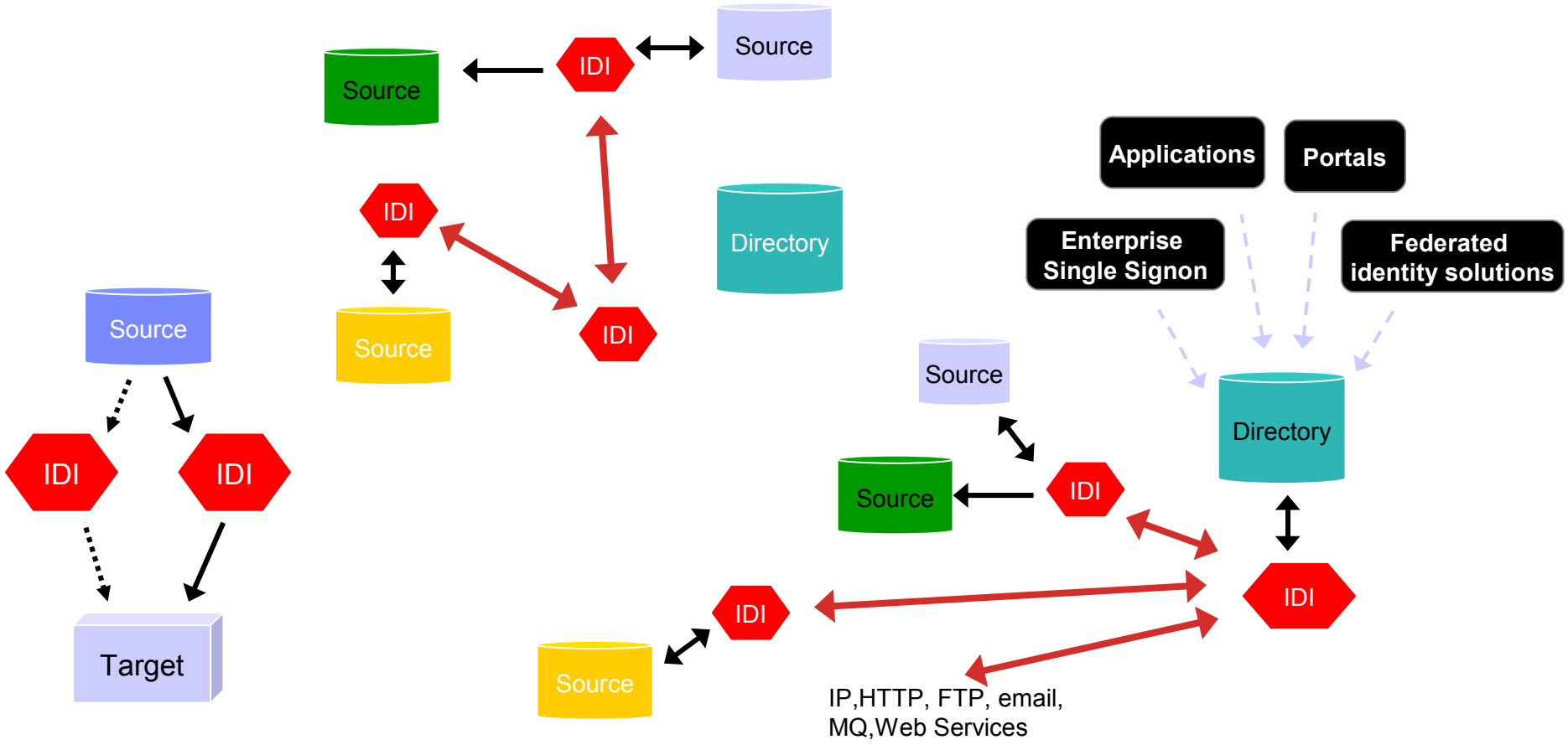
Interpreta y transforma el flujo de datos en el formato deseado

IBM Tivoli Directory Integrator: Un ejemplo

- Un usuario se registra en una APP que usa una BBDD SQL como repositorio de usuarios
- El mismo usuario, con un uid diferente, existe en una directorio LDAP.
- Queremos registrar al mismo usuario en un portal y necesitamos un formulario XML, con los datos de registro de la aplicación y algunos datos que ya están en el directorio LDAP
- Input BBDD, LDAP
- Output documento XML



IBM Tivoli Directory Integrator: aplicable a escenarios sencillos o realmente complejos



ITDI - Caracteristicas Fundamentales

Extremadamente Flexible

Arquitectura de bloques de construcción que combina componentes standard y scripts de escasa complejidad

Pequeño y Escalable

Compacto, multi-threaded & puede desplegarse en entornos distribuidos

Independiente de plataforma

Soporta Unix, Linux, Solaris, NT , Windows, HP-UX, IBM AIX

Basado en Standards

XML, así como los formatos y protocolos standards para Internet, mensajería, LDAP, BBDD y web services standards

Intuitivo y facil de usar

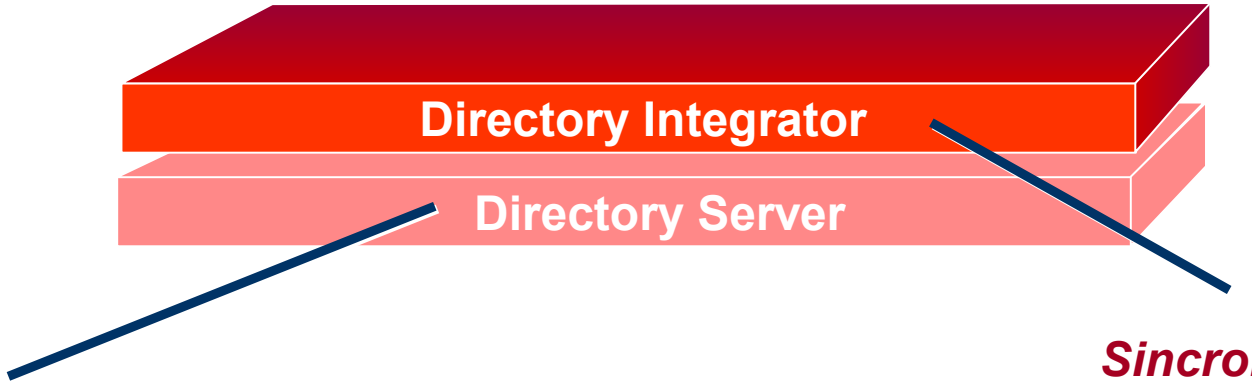
Desarrollo de soluciones guiada paso a paso, con ciclos de desarrollo-prueba-despliegue Muy cortos

Integración NO intrusiva

Los conectores no afectan a los datos ni al flujo en en el origen

ITDI – IBM Tivoli Directory Integrator

BAJO COSTE
EXTREMADAMENTE FLEXIBLE
NO INTRUSIVO

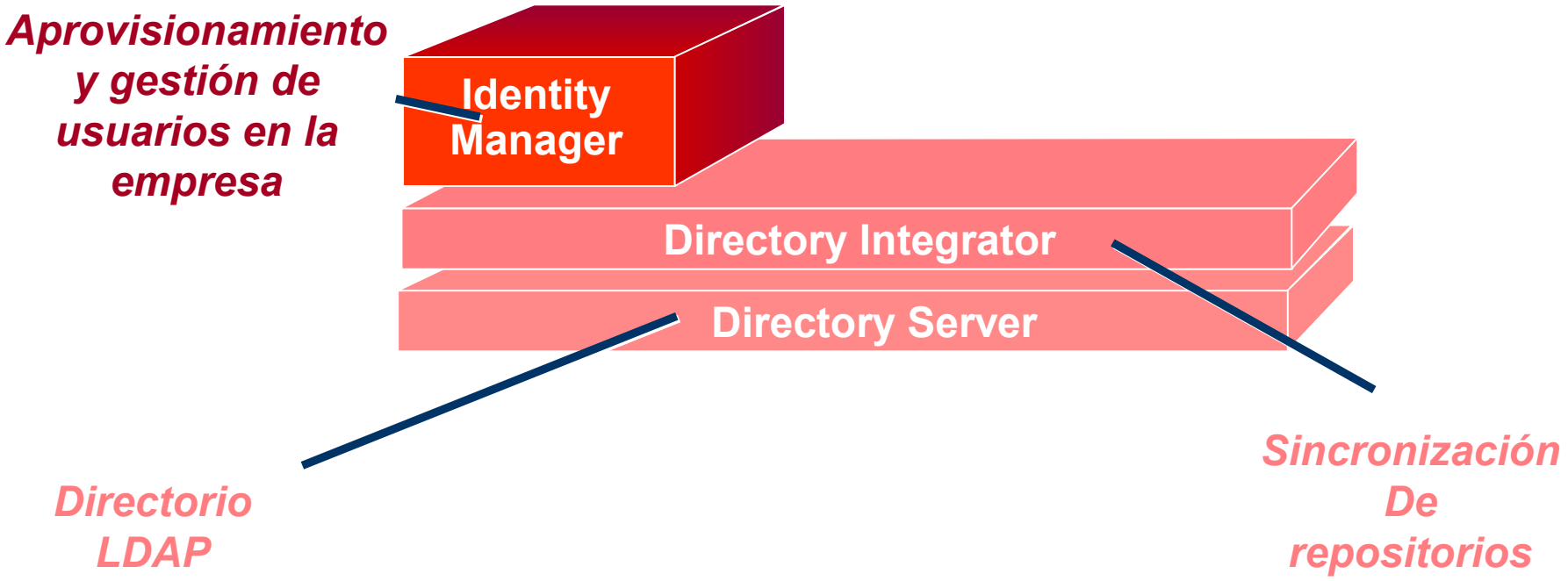


Directorio LDAP

Sincronización De repositorios

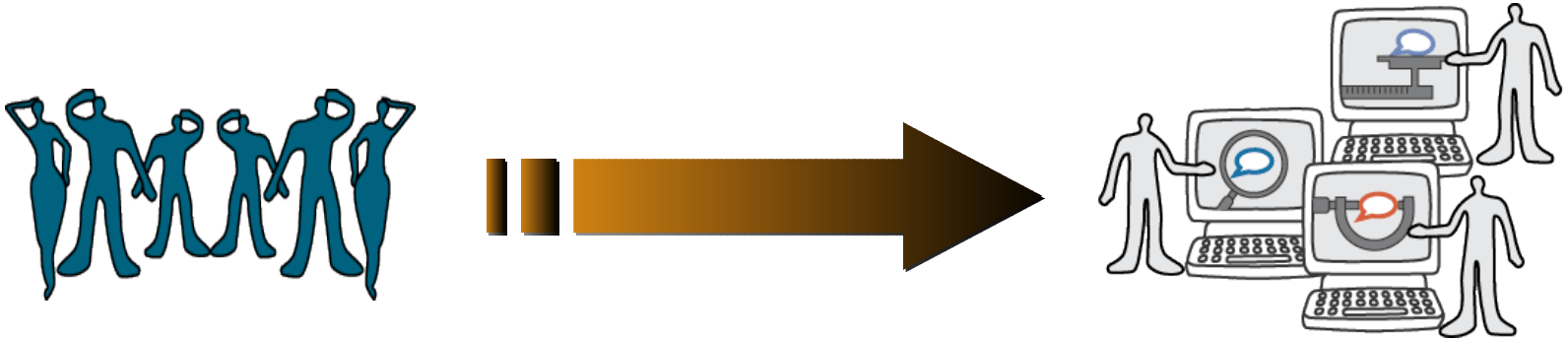
ITIM – IBM Tivoli Identity Manager

Gestión integral de identidades, cuentas y contraseñas. Automatización de la gestión de su ciclo de vida. Auditoria y gestión de políticas de identidad



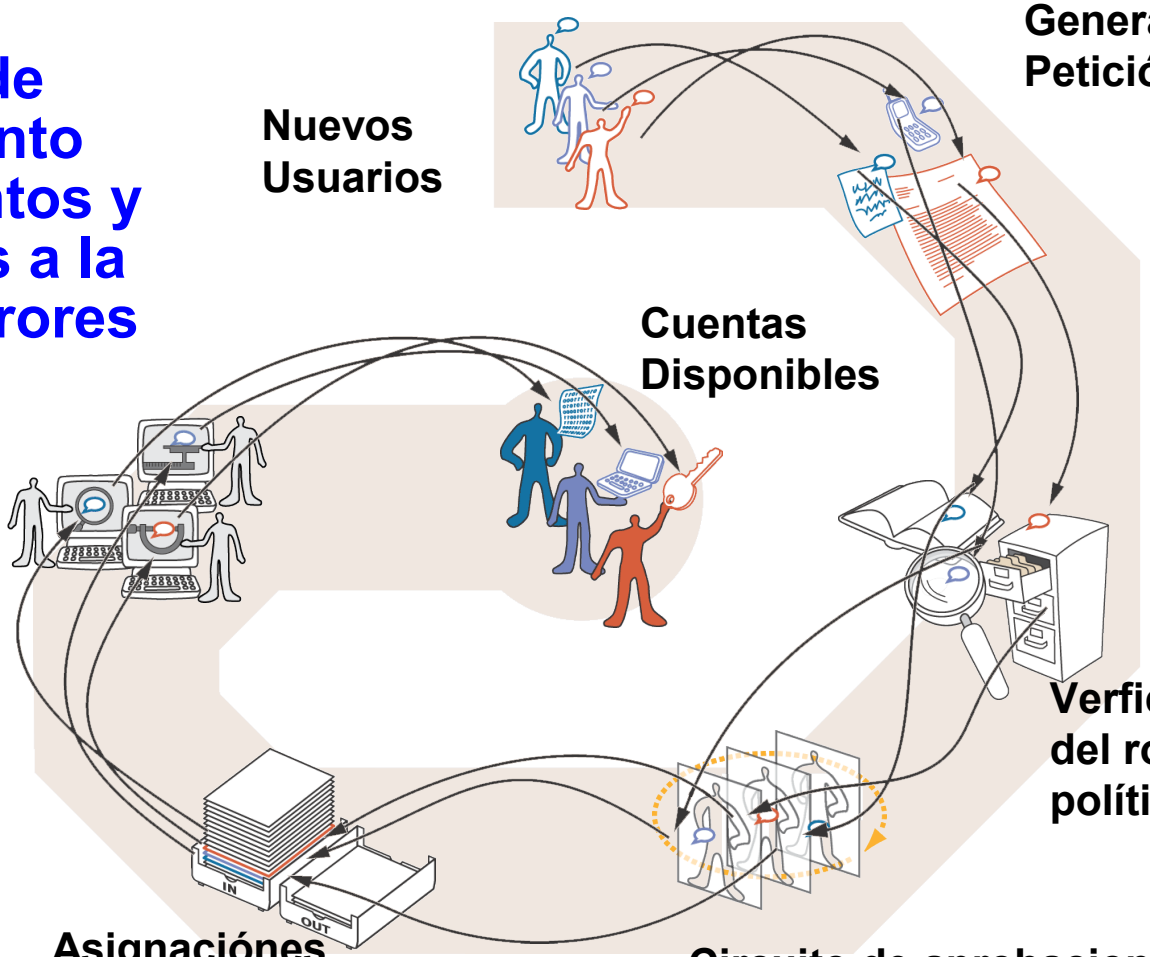
La gestión de identidades conecta personas con los recursos IT necesarios para ser productivos

Para cada usuario -> Conocer a que recursos tiene acceso
Para cada recurso -> Conocer que usuarios son válidos
Garantizar que una persona tiene acceso a los recursos que necesita y solo a los que necesita



Problemática de Aprovisionamiento

Los procesos de aprovisonamiento manual son lentos y mas propensos a la comisión de errores



Necesidades Derivadas

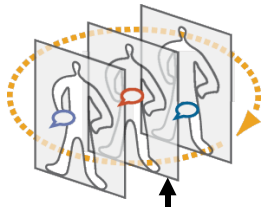
- Necesidad de auto-servicio para reducir/eliminar costes en el help desk
- Necesidad de conocer los permisos y derechos de acceso de todos los usuarios en las distintas plataformas y aplicaciones
- Necesidad de desactivar facil y rápidamente usuarios cuando dejan de pertenecer a la organización
- Necesidad de automatizar en el mayor grado posible, los procesos de alta de usuarios en las distintas plataformas y aplicaciones
- Necesidad de mantener un registro centralizado de los cambios en el tiempo de permisos y derechos de acceso de los distintos usuarios
- …

Tivoli Identity Manager facilita la gestión de identidades

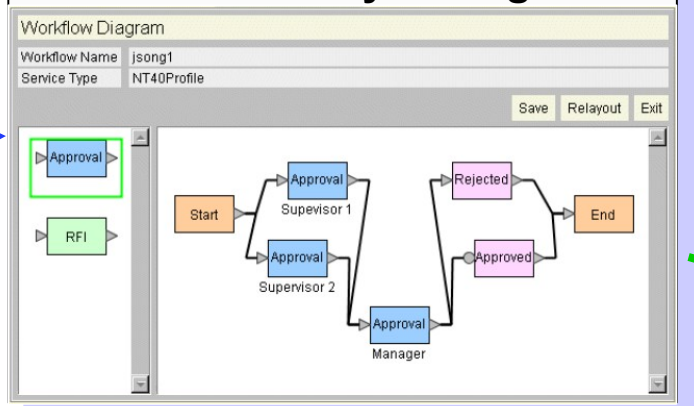
Cambio en personal(add/del/mod) → Evaluación políticas de acceso → Circuito de aprobación → Actualización cuentas

Detecta y corrige privilegios establecidos localmente

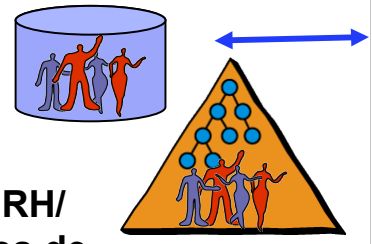
Aprovisionamiento basado en Politicas para toda la infrastructura IT



Tivoli Identity Manager



Gestión de cuentas en 70 tipos distintos de sistemas, aplicaciones de negocio, portales, etc

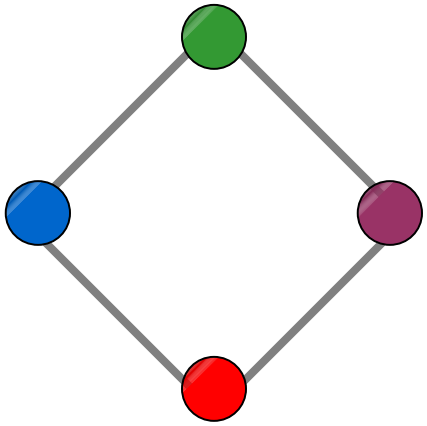


Sistemas RH/ Repositorios de Usuarios

IBM Tivoli Identity Manager – Retorno de la Inversión

Disminución de costes de administración

Mejora de los tiempos de respuesta y niveles de disponibilidad/productividad

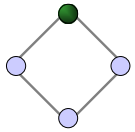


Soporte de políticas y normativas relacionadas con la gestión de usuarios

Incremento de la Seguridad

Automatización de la gestión de los privilegios y atributos de los usuarios y la eliminación de errores en los procesos

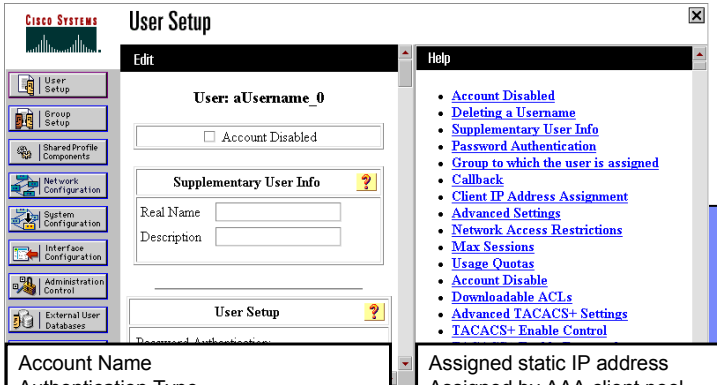
Reducción Costes Administración



Proceso manual:

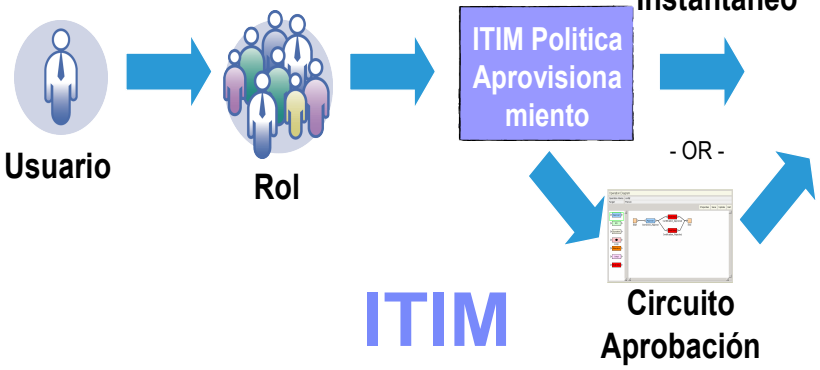
Lento, propenso al error

…Generación, actualización y eliminación automática de privilegios y derechos de acceso



Account Name
Authentication Type
Group Name
Authentication PAP password
Separate password flag
Secondary CHAP password
User Field 1 – Real Name
User Field 2 - Descriptiion
User Field 3 –
User Field 4 –
User Field 5 –
Callback type
Callback number
Client IP Address Assignment type

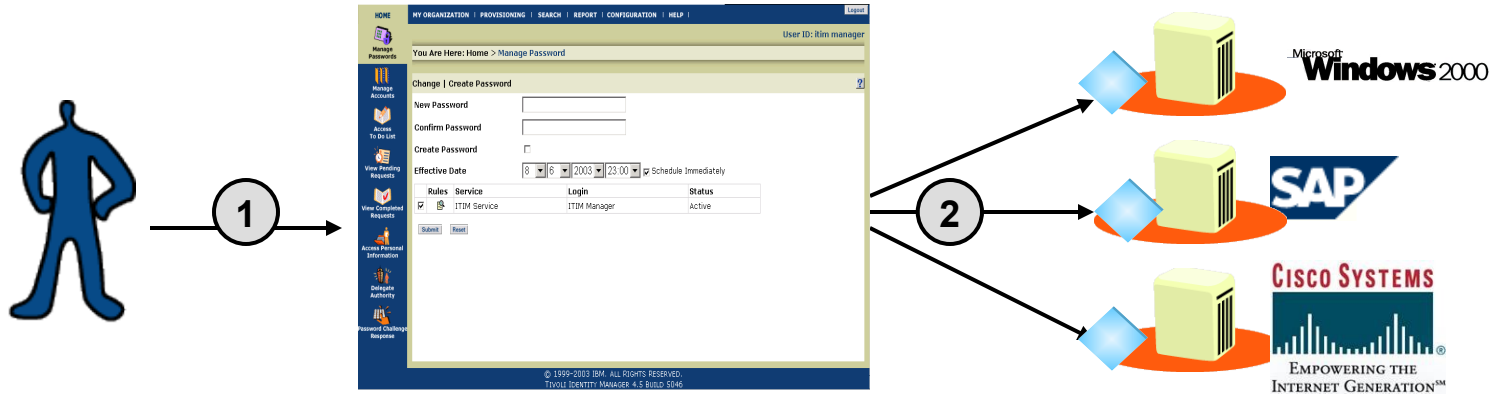
Assigned static IP address
Assigned by AAA client pool
Max sessions type
Number of sessions
Account Disable type
Date exceeds
Fail attempts
IP-based access restrictions
Table (AAA Client,port,address)
CLI/DNIS-based access restrictons
Table (AAA Client,port,CLI,DNIS)



Reducción
Costes
Administración

Autogestión de Contraseñas. Disminución de costes de Help-desk y mejora del servicio para el usuario final

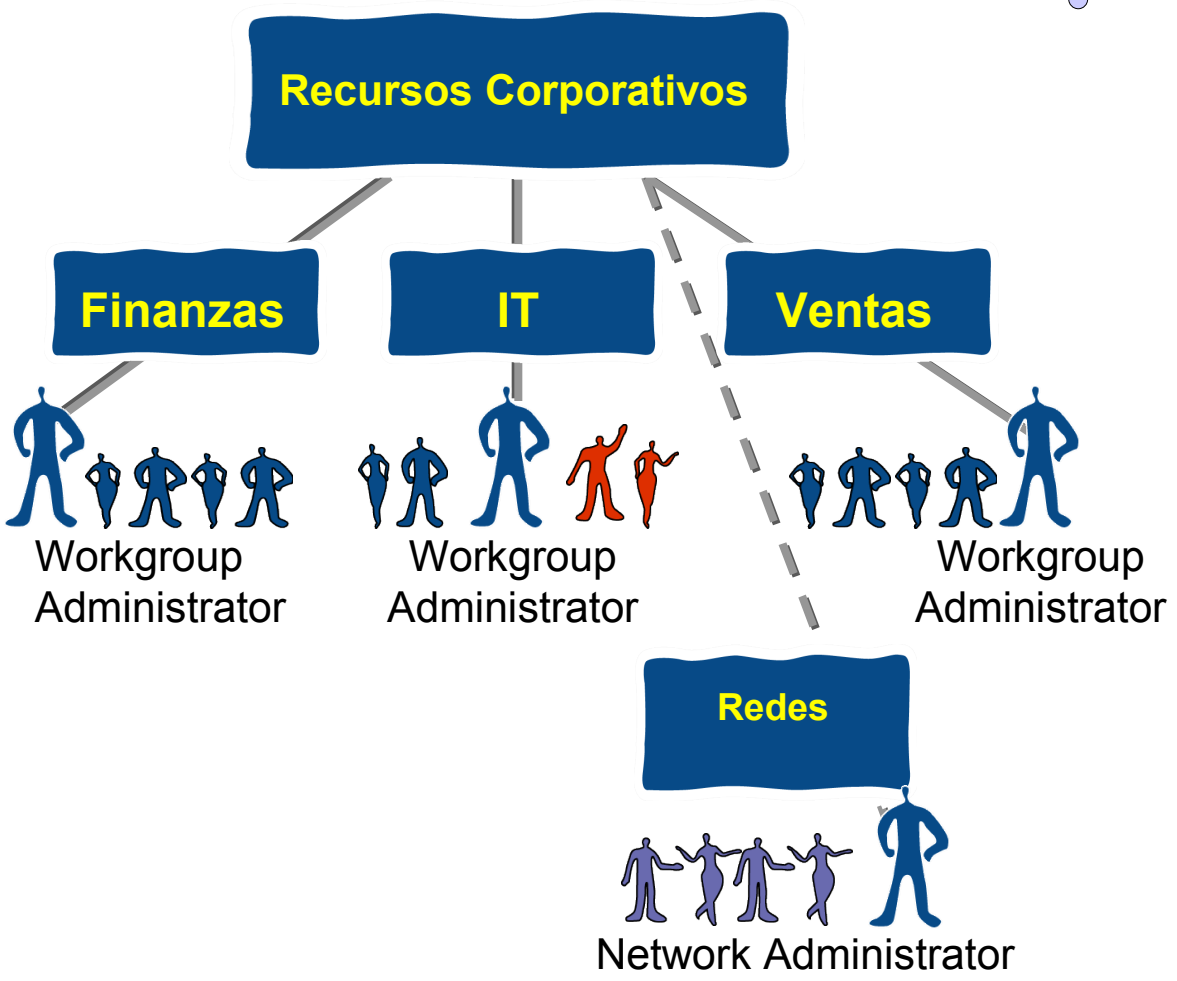
- Auto servicio de reset de contraseñas en todos los sistemas
- Sistema de preguntas-reto para la recuperación de contraseñas
- Sincronización de contraseñas e IDs
- Verificación de políticas de contraseña



Reducción Costes Administración

Administración Delegada

- **Centralización donde tiene sentido: (80% de los casos)**
  - Políticas Corporativas
  - Tareas comunes de administración
- **Delegar el control al responsible específico en áreas específicas**
  - Dominios, aplicaciones concretas, etc



Respuesta rápida a peticiones temporales de acceso y revocación automáica

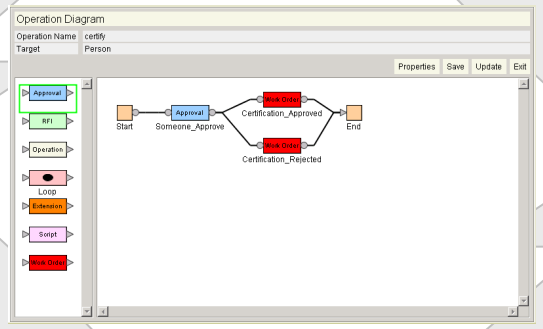
Mejora Tiempos Respuesta

Usuario nuevo / Auto-Registro

Acceso temporal a la red para un proveedor

Re-certificación de la necesidad

Proceso definido por la compañia



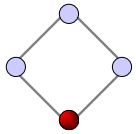
Crea
Añade

Borra
Modifica

- Cuenta
- Notif.
- Politica
- Rol
- Usuario
- Ext Sys

Tivoli Identity Manager Workflow

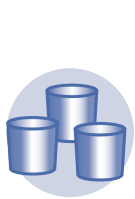
Identificación de “cuentas huerfanas” relacionando personas con cuentas de usuario automáticamente



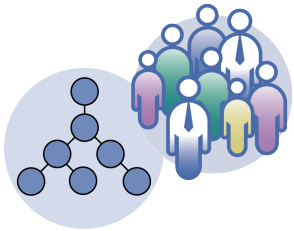
Incremento seguridad

Entre el 30% y el 60% de las cuentas en un sistema son huerfanas

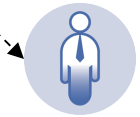
Gartner Group



Fuente Autorizada de identidades (Habitualmente RRHH)



TIM Repositorio identidades



John C. Doe

Sarah K. Smith

Cuentas

jcd0895

jdoe03

Sarah_s4

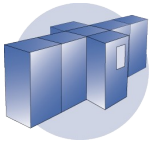
nbody

ackerh05

doej

smiths17

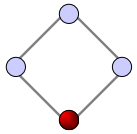
Aplicaciones de negocio



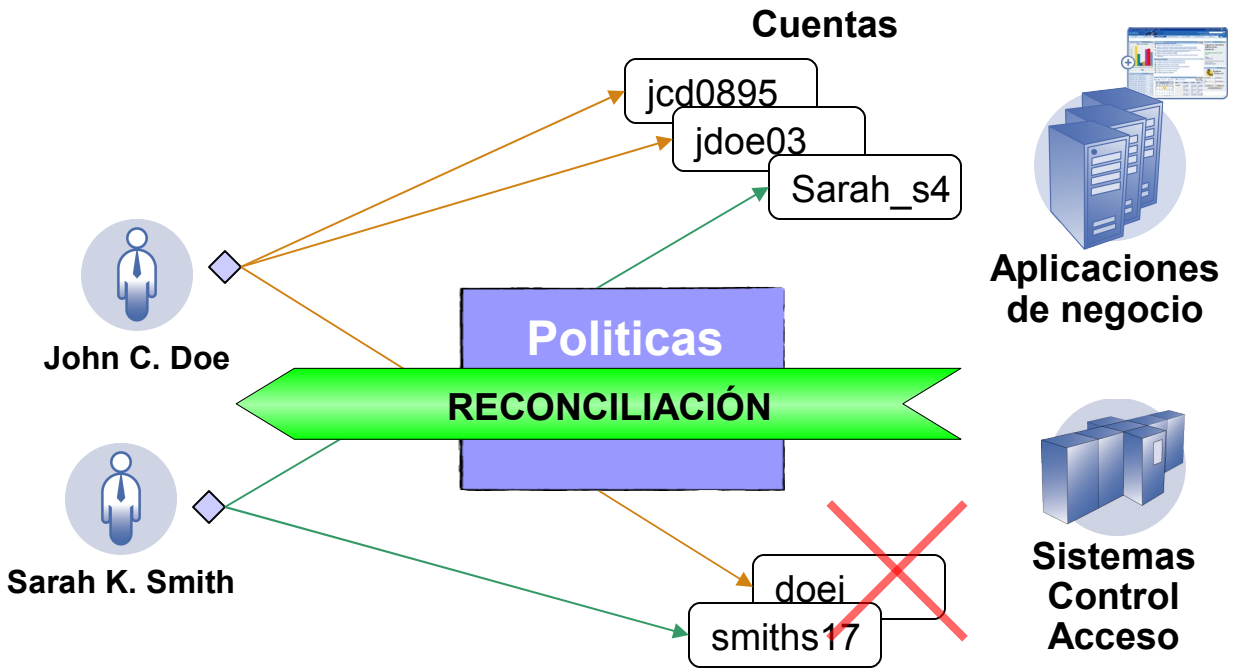
Sistemas Control Acceso

TIM permite ignorar, borrar, deshabilitar automáticamente o implementar un workflow para tratar las cuentas huérfanas

El Proceso de reconciliación identifica las cuentas que no se ajustan a las políticas definidas

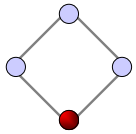


Incremento seguridad



TIM permite ignorar, borrar, deshabilitar o corregir automáticamente o implementar un workflow para tratar las cuentas que no se ajustan a las políticas definidas

Automatización de la expiración de contraseñas y politicas recertificación de cuentas integradas con el workflow y los mecanismos de notificación



Incremento seguridad

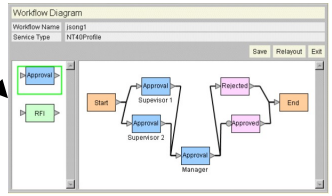
Tivoli software **Identity Manager**

Recordatorios de expiración de contraseñas

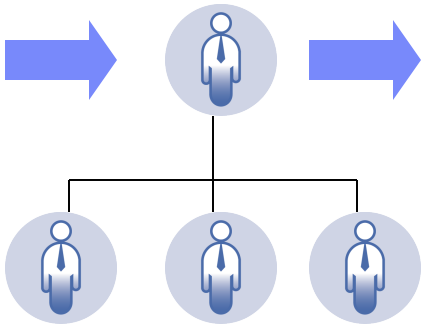
Cambio de contraseña

-o-

Bloqueo de cuenta



Workflow de re-certificación



Renovación de cuenta

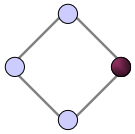
-or-

Negación de acceso

Disparador de Politicas:

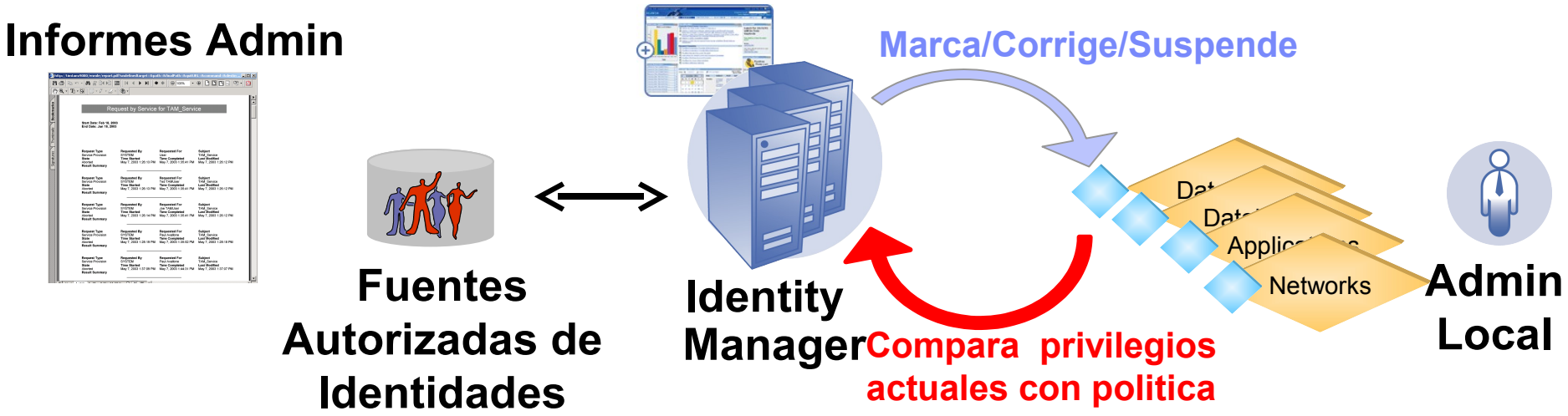
- Fecha
- Antiguedad
- Cambio en un atributo
- Combinación de las anteriores

Repositorio Centralizado de de identidades y cuentas
Facilitador para el despliegue de políticas corporativas

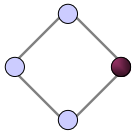


Soporte
Regulacion
Normativas

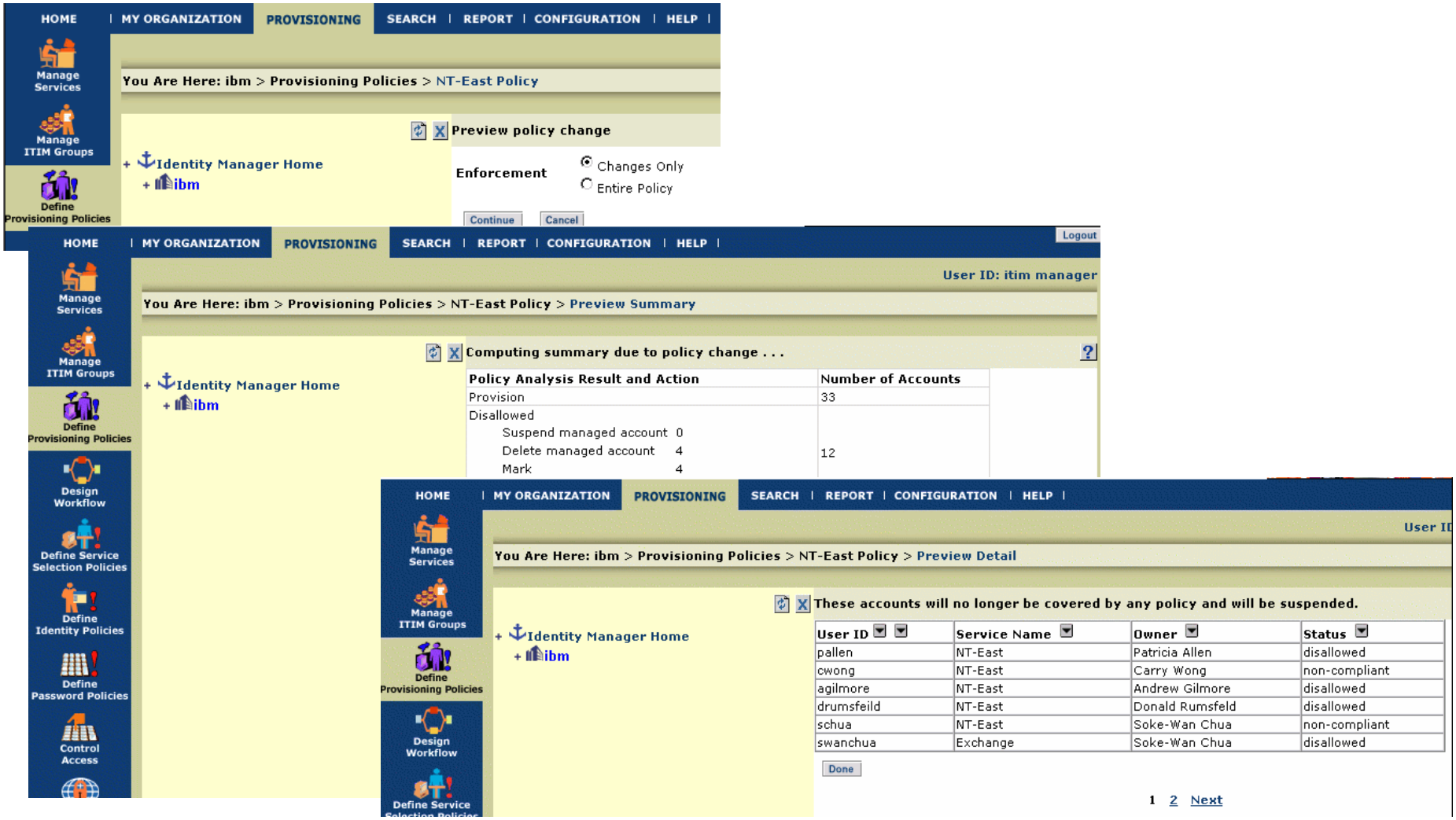
- Repositorio centralizado con los datos de identidad y cuentas de las personas de la identidad. Auditoria de privilegios
- Facilitador para el despliegue e imposición de políticas
- Registro de las operaciones de administración. Auditoria de operaciones



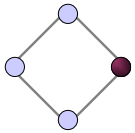
Simulación de políticas y ejecución en modo borrador. Conocer el impacto de la política antes de desplegarla



Soporte
Regulacion
Normativas

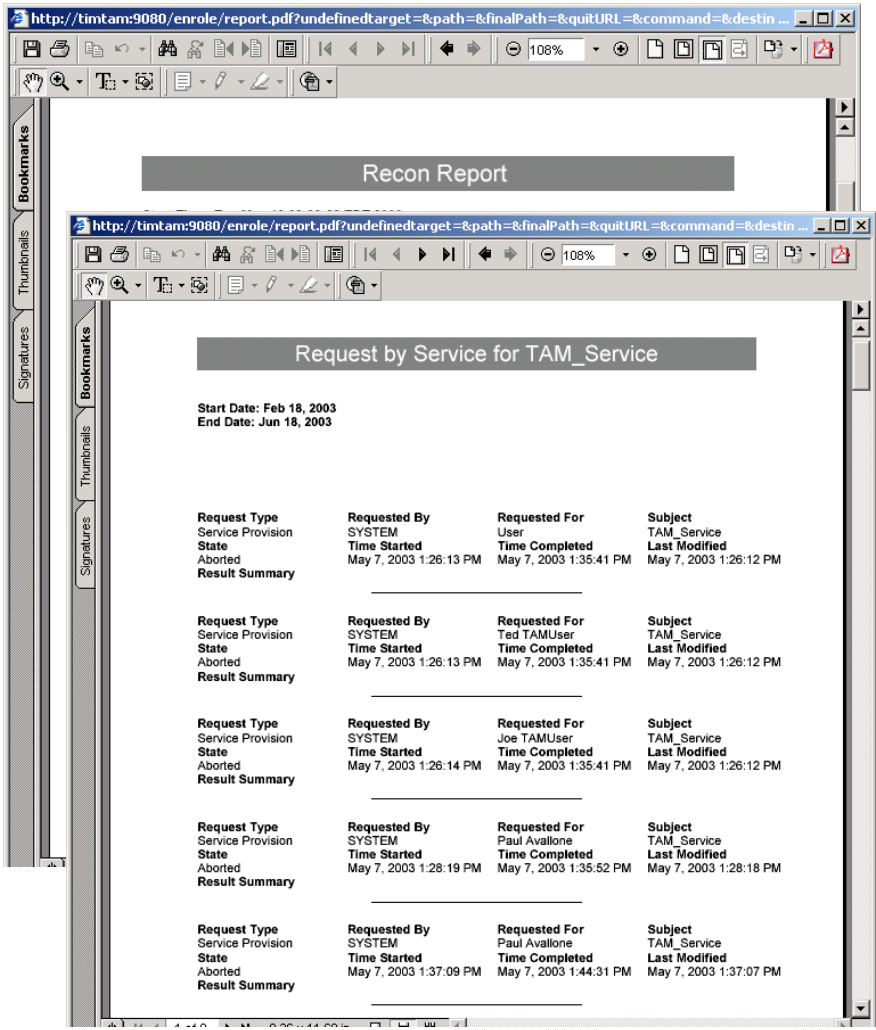


Obtención rápida de informes



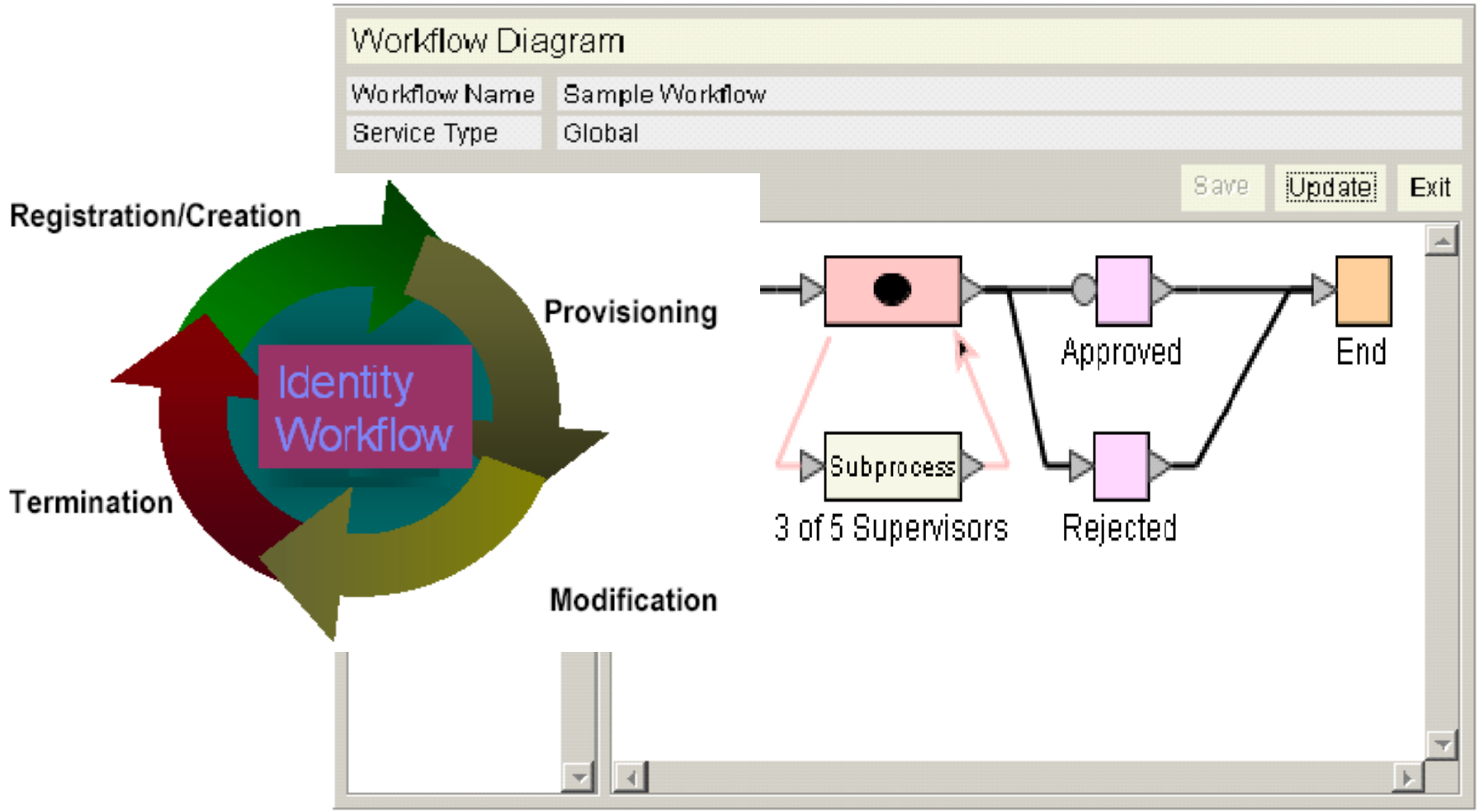
Soporte
Regulacion
Normativas

- Informes predefinidos o generados por el administrador
- Visión centralizada de personas y privilegios
- Control de derechos de acceso por persona
- Control de derechos de acceso por recurso
- Informes en formato Acrobat
- Soporte e Integración de Crystal Reports



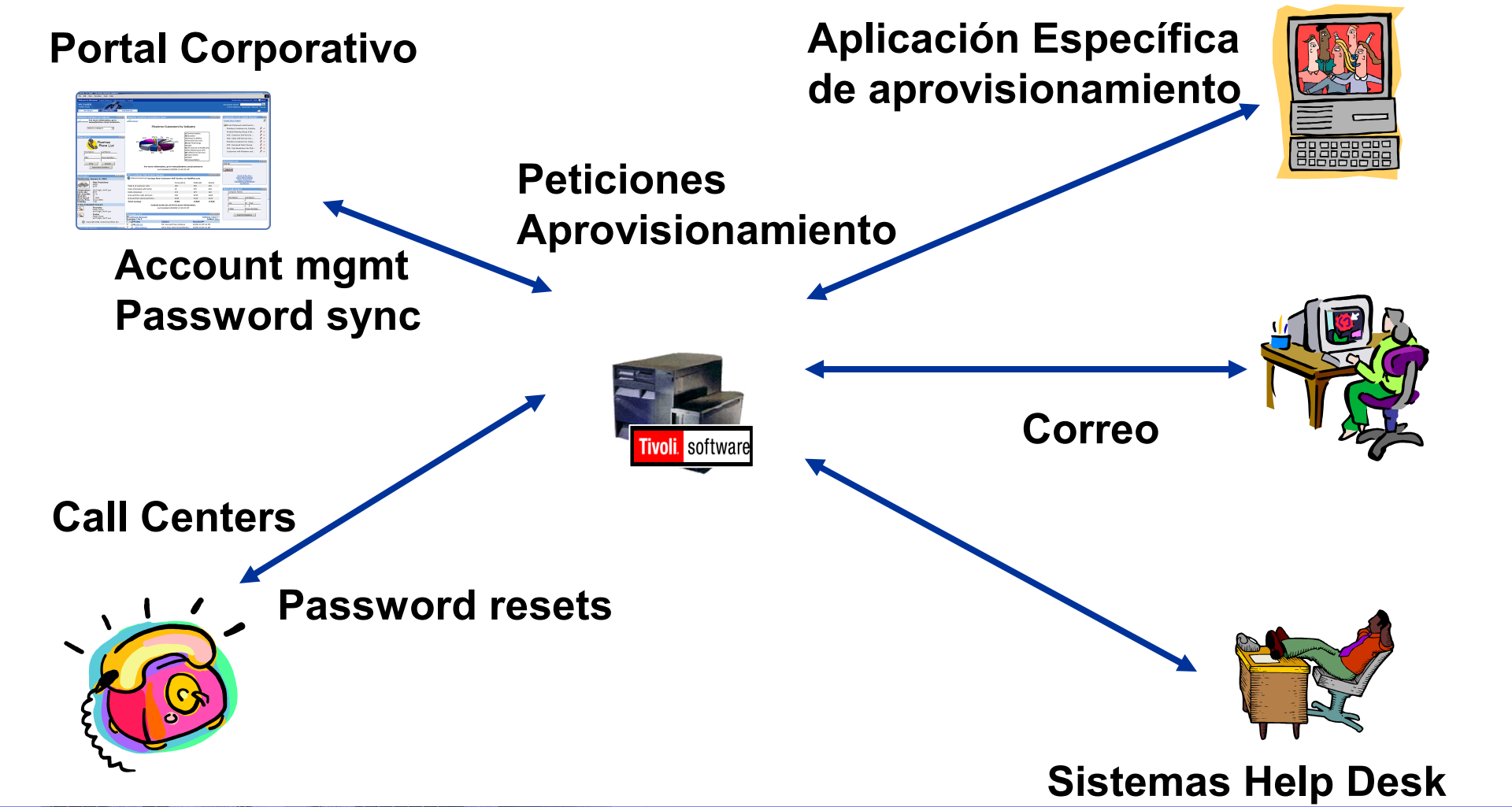
IBM Tivoli Identity Manager

Extremadamente Flexible, cada operación concebida como un workflow modificable



IBM Tivoli Identity Manager

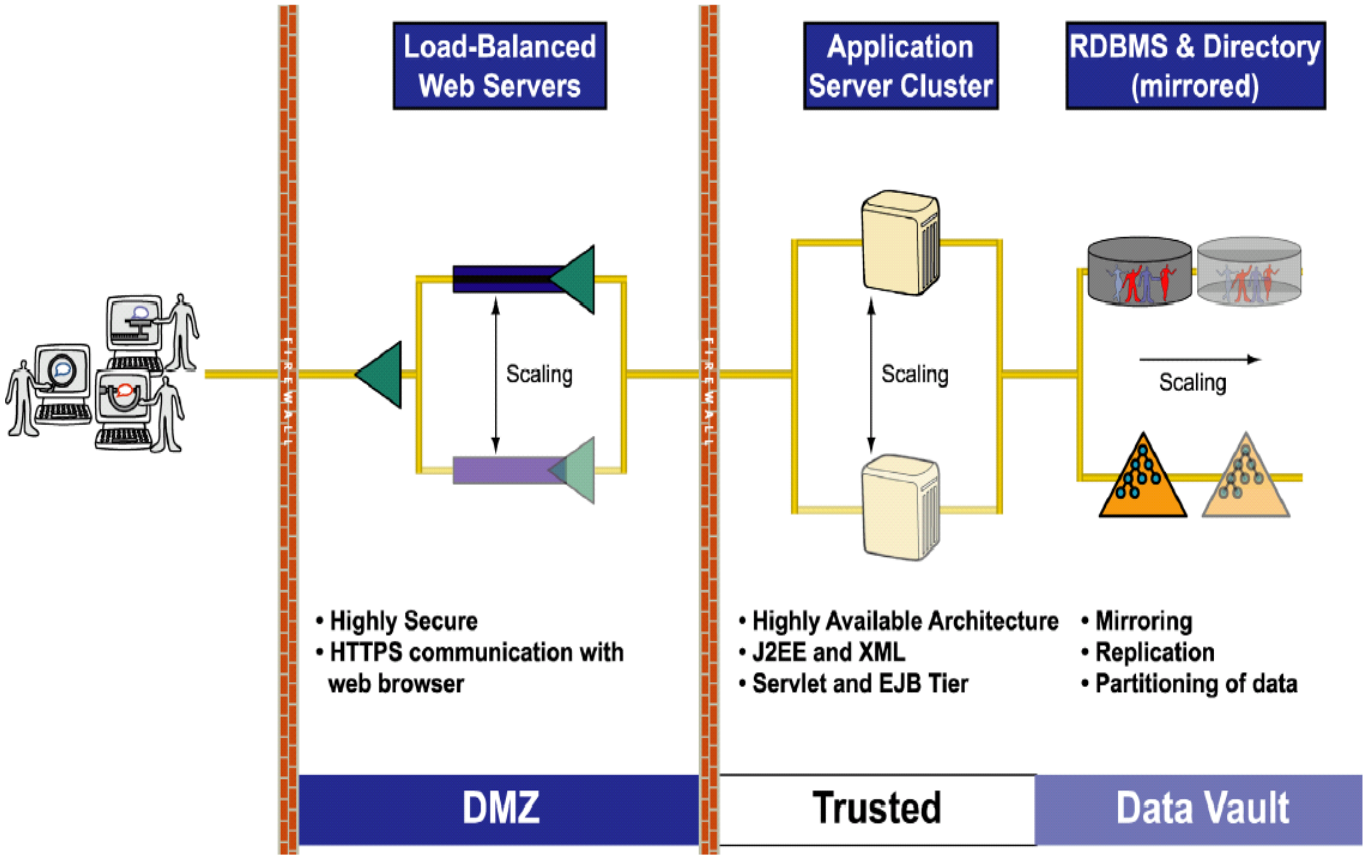
Facilmente integrable, APIs Java de operación y administración permiten la integración con otros sistemas



IBM Tivoli Identity Manager
Arquitectura escalable

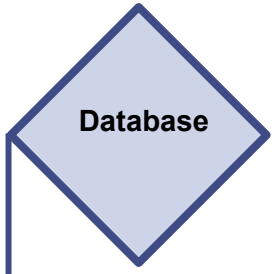
Single server

Alta Disponibilidad, multi-server



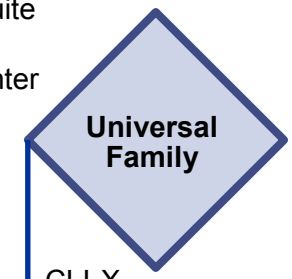
IBM Tivoli Identity Manager
Amplia cobertura de Agentes

CA - ACF2
CA - Top Secret
Entrust PKI
Entrust getAccess
MVS RACF
Netegrity SiteMinder
Oblix NetPoint
Remedy*
RSA ACE/Server
RSA ClearTrust
Tivoli Access Manager*



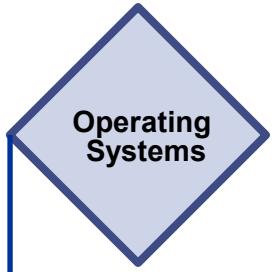
IBM DB2/UDB*
Informix*
Oracle 8/8i/9i*
SQL Server*
Sybase*
Teradata DBMS*

Cisco ACS
Clarify eFrontOffice*
Documentum*
Lotus Notes*
MS-Exchange*
Novell e-Directory*
Novell GroupWise*
Oracle E-Business Suite
PeopleSoft
Peregrine ServiceCenter
SAP EP6
SAP R/3*
Siebel



CLI-X
LDAP-X*
- Critical Path Injoin
- IBM Directory Server
- Oracle OID
- Sun iPlanet Directory

RDBMS-X*
Universal Provisioning Agent*



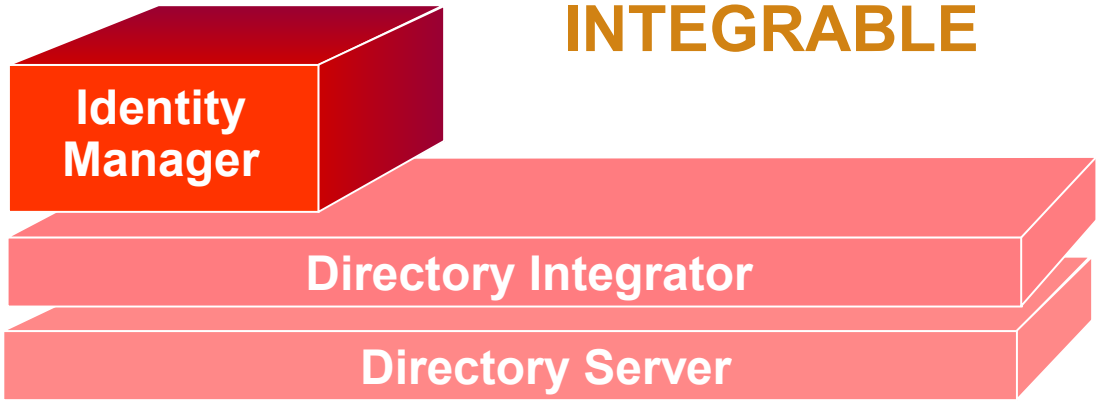
HP/Compaq Tru64
HP-UX
IBM AIX
IBM AS/400
OpenVMS
RedHat Linux
Sun Solaris
SuSE Linux
Windows 2000*
Windows NT*

Design Characteristics:
- **Secure**
- **Bi-directional**
- **Firewall friendly**

*** Offers remote operation**

TIVOLI IDENTITY MANAGER

POTENTE
FLEXIBLE
ESCALABLE
INTEGRABLE



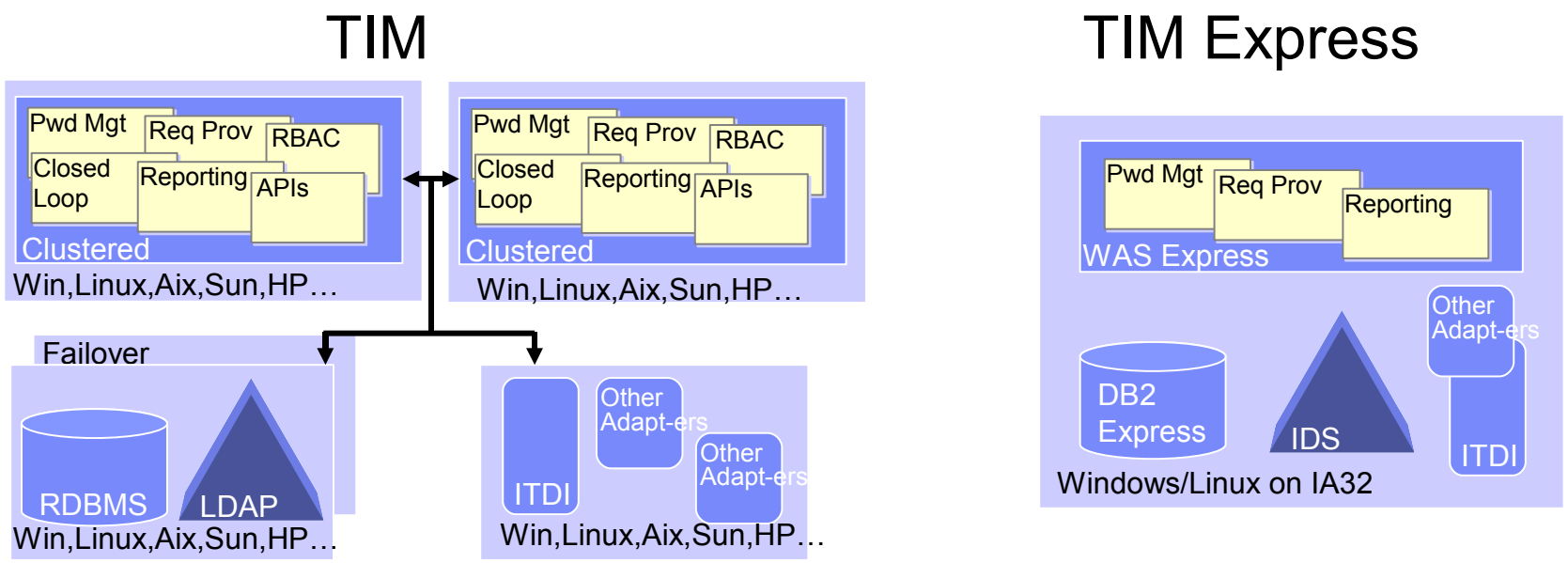
También disponible TIM Express

Instalación mas simple, despliegue mas rápido

Numero de usuarios limitado a 5000

Incorpora “best-practices”

Especialmente orientado a pequeña mediana empresa

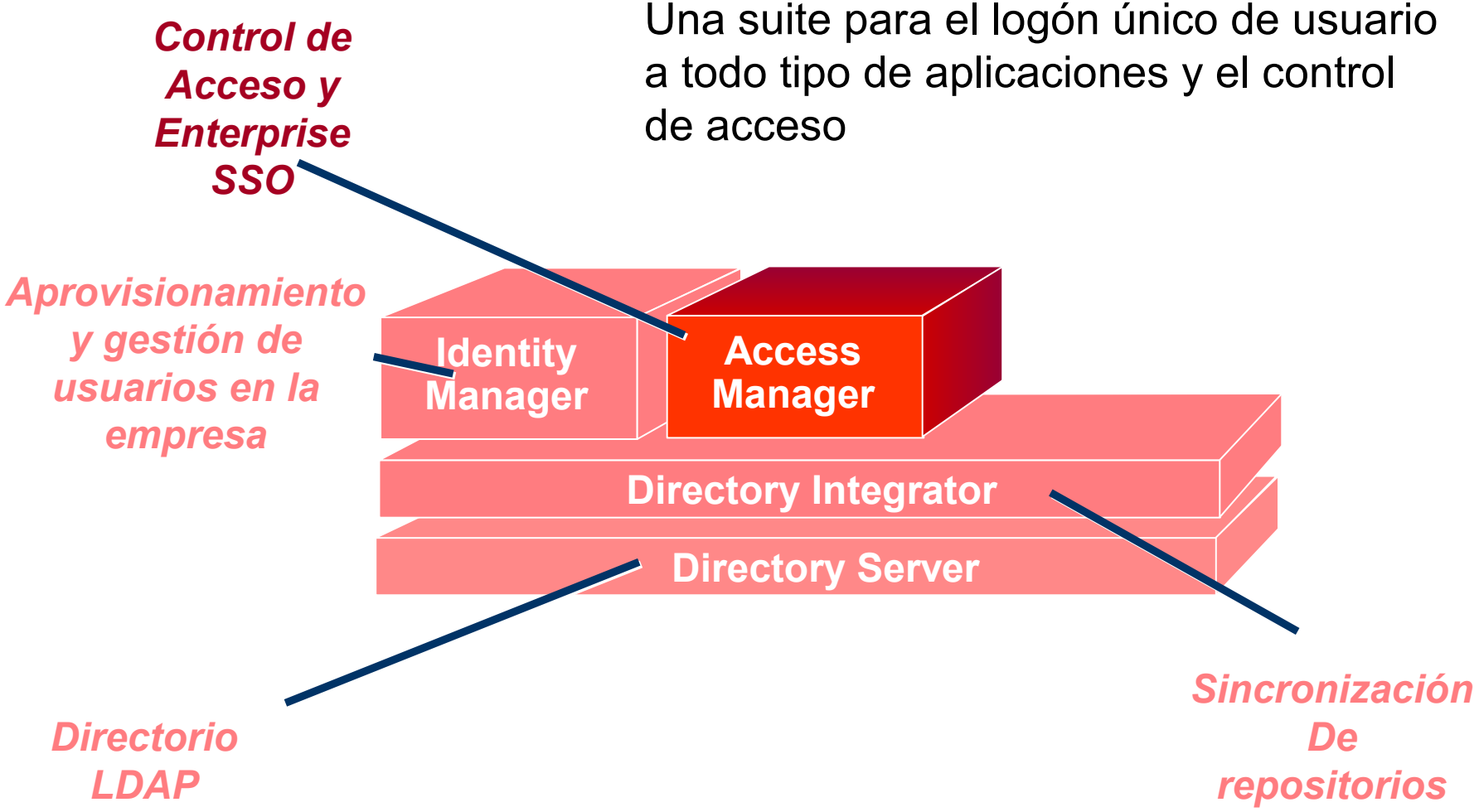


TIM versus TIM Express

	TIM Express	TIM 4.6
Arquitectura y configurabilidad	**Servidor único**, no clustering **Instalación simple**	Clustering, Arquitectura flexible, múchas opciones de configuración
Aprovisionamiento	Autoservicio y aprovisionamiento bajo demanda. Des-aprovisionamiento manual	Aprovisionamiento y des-aprovisionamiento bajo demanda y automático, basado en roles
Políticas	Recertificación para detectar y desactivar cuentas no acordes	Identificación, corrección y/o des-activación automática de cuentas no-acordes, Worlflow de recertificación.
Auditoria	Reports standard	Reports a medida integración Cristal Reports
Customization	Limitada, incorpora best practices	Workflows modificables, APIs de integración
Escalabilidad	Max 5,000 usuarios	Capaz de gestionar cientos de miles
Plataformas	Linux y Windows en xSeries	Windows, Linux,Aix,HP, etc

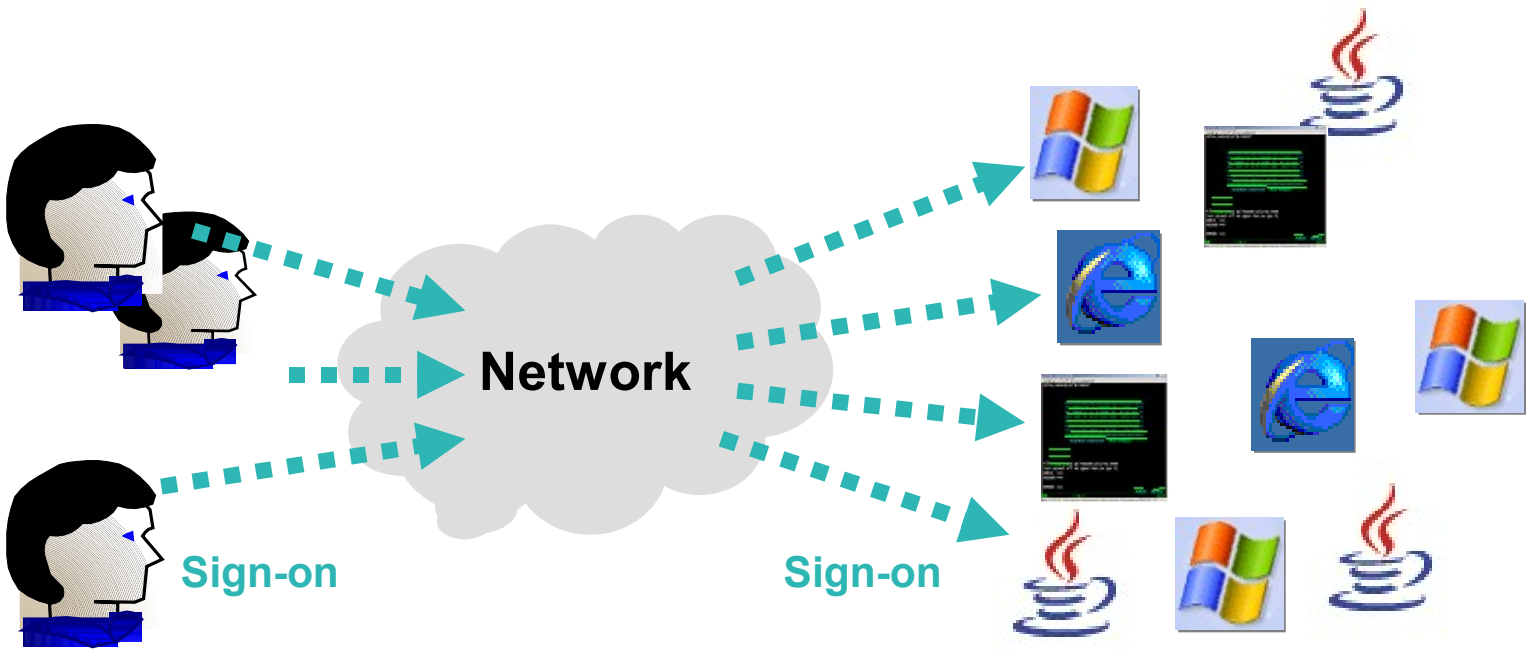
ITAM – IBM Tivoli Access Manager

Una suite para el logón único de usuario a todo tipo de aplicaciones y el control de acceso



TAM–ESSO -> Logon unico a todo tipo de aplicaciones

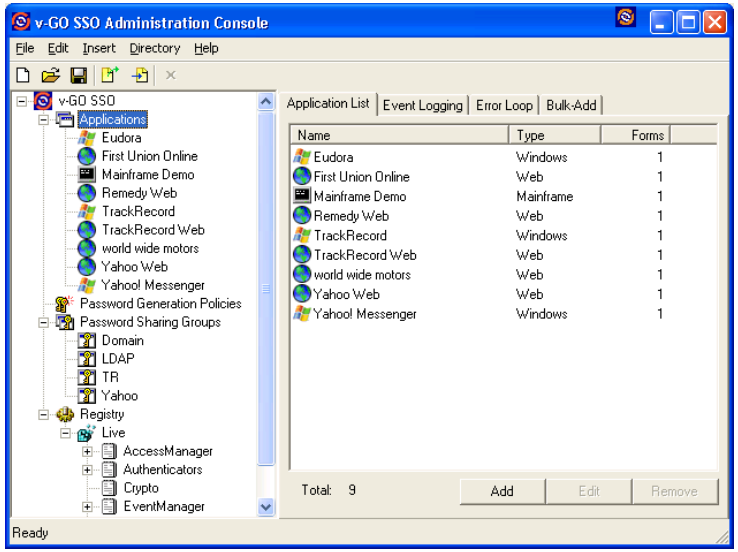
- Simplificación de la experiencia del usuario final,
- El usuario se autentica una sola vez, T-ESSO responde (autentica al usuario) a los sistemas finales cuando el usuario accede un recurso que solicita autenticación.



Tivoli Access Mgr for Enterprise Single Sign-on

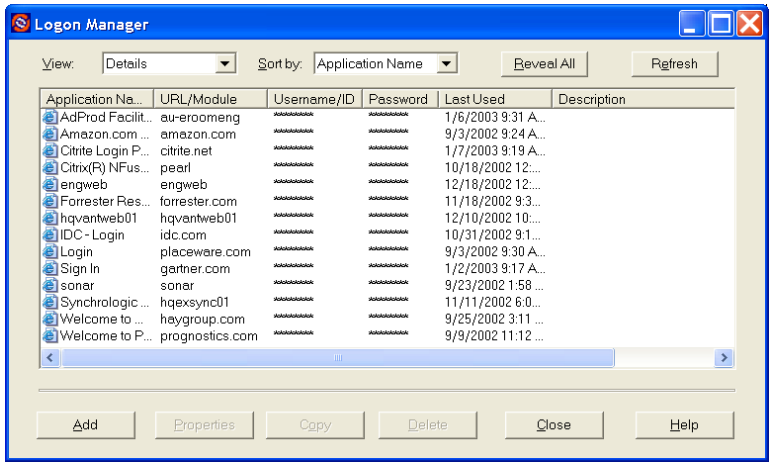
- Implementa el login y cambio de contraseña para todo tipo de aplicaciones Web, Java y de terminal.
- No require modificaciones en los sistemas finales => despliegue rápido y no intrusivo.
- Se soportan distintos tipos de autenticación primaria (la única que realiza el usuario): basada en el logon de Windows, smart cards, dispositivos biométricos, certificados digitales, etc.
- Generación automática de contraseñas y soporte de políticas de contraseña.
- Soporta distintos modos de operación: connectado, desconnectado, multi-puesto y modo “kiosko”
- Sincronización inteligente de credenciales con repositorio central o token.
- Credenciales cifradas en todo momento, permitiendo seleccionar el algoritmo (3DES, AES etc.), solo la credencial utilizada se desencripta en le momento de ser utiizada.

Componentes básicos

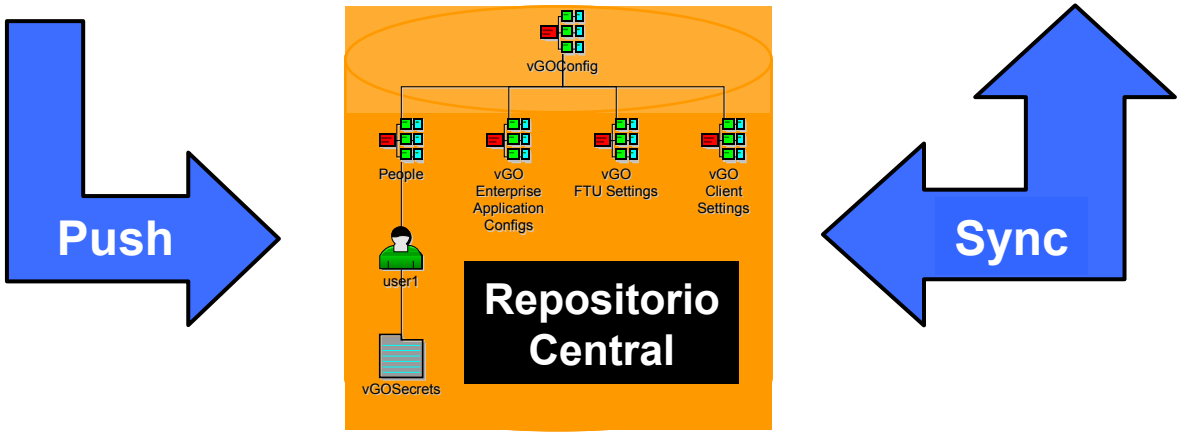


Administration Console

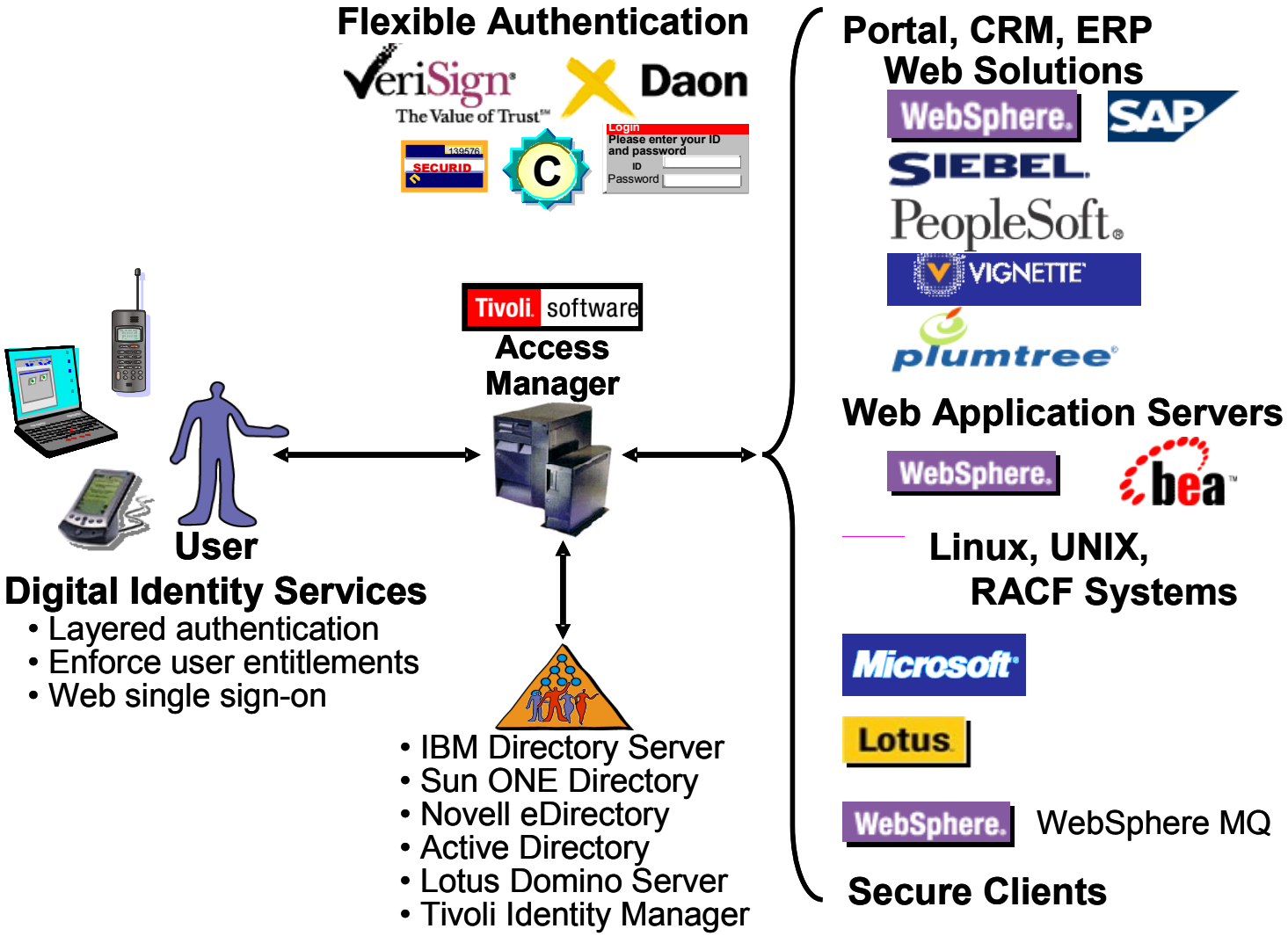
Agente Local - Desktop



SSO Agent

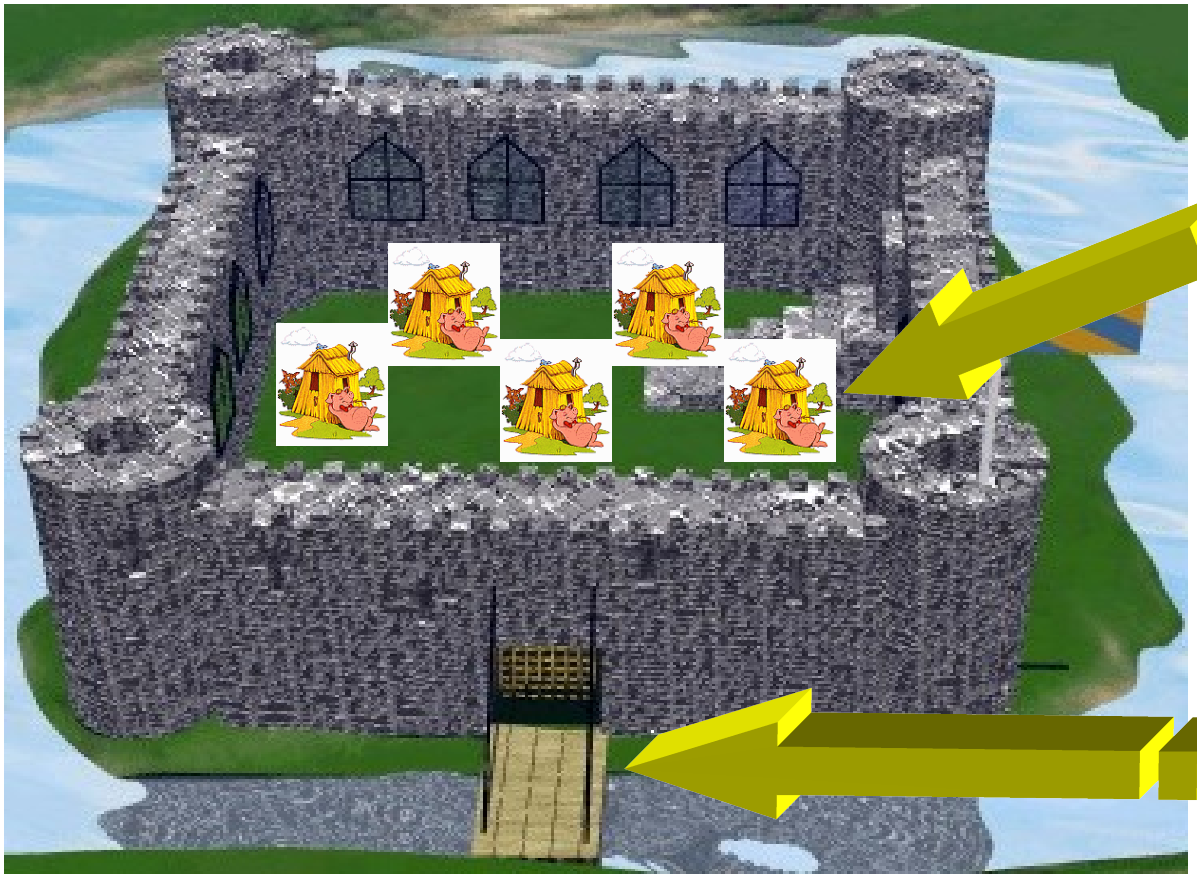


Tivoli Access Manager for eBusiness



Seguridad en Aplicaciones Web — Modelo Corportaivo

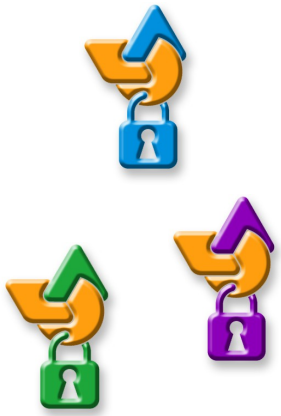
Best Practice: Mover la autenticación y la autorización a la “frontera exterior” de la red



Aplicaciones protegidas por dispositivos de seguridad perimetral

Un único punto de acceso a las aplicaciones corporativas

Beneficios del modelo de servicios comunes de Seguridad



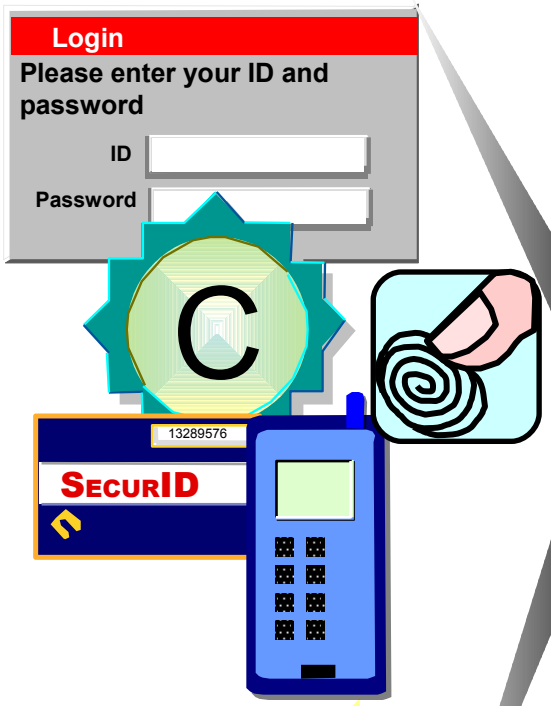
Modelo Habitual

- Seguridad embebida en cada aplicación
- Las políticas de acceso neceista actualizarse en múltiples repositorios
- Login independiente a cada aplicación

Con Tivoli Access Manager

- Servicios comunes de seguridad, separados de las aplicaciones
- Administración comun y delegable
- Single sign-on

Autenticación



Soporte de multiples metodos de autenticación

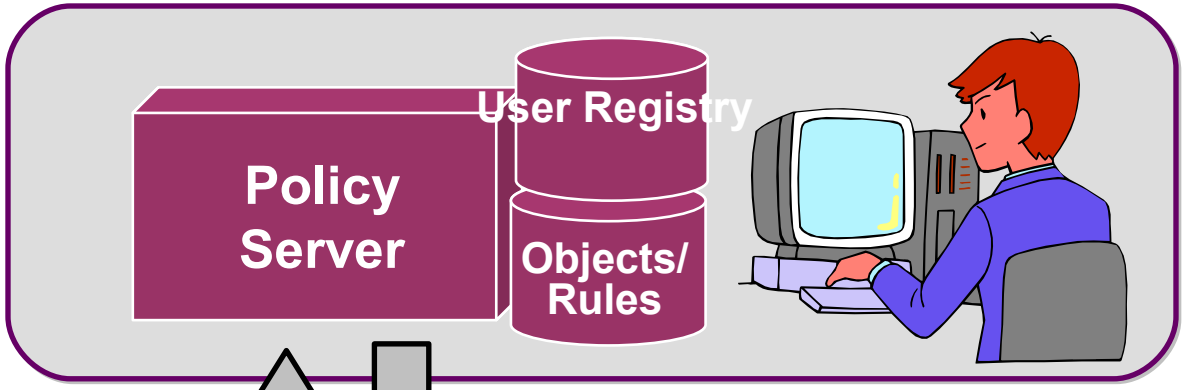
múltiples opciones de Web SSO:

Access Manager

- *iv-user HTTP Header*
- *basicauth HTTP Header*
- *Forms-based SSO*
- *Lightweight Third-Party Authentication (LTPA)*
- *Trust Association Interceptor*
- *GSO Junction*
- *Desktop SSO with initial sign-on to MS NTLM/Kerberos*

WebSphere
PeopleSoft
SIEBEL
Microsoft
Lotus
VIGNETTE
SAP
& more

Modelo de Autorización



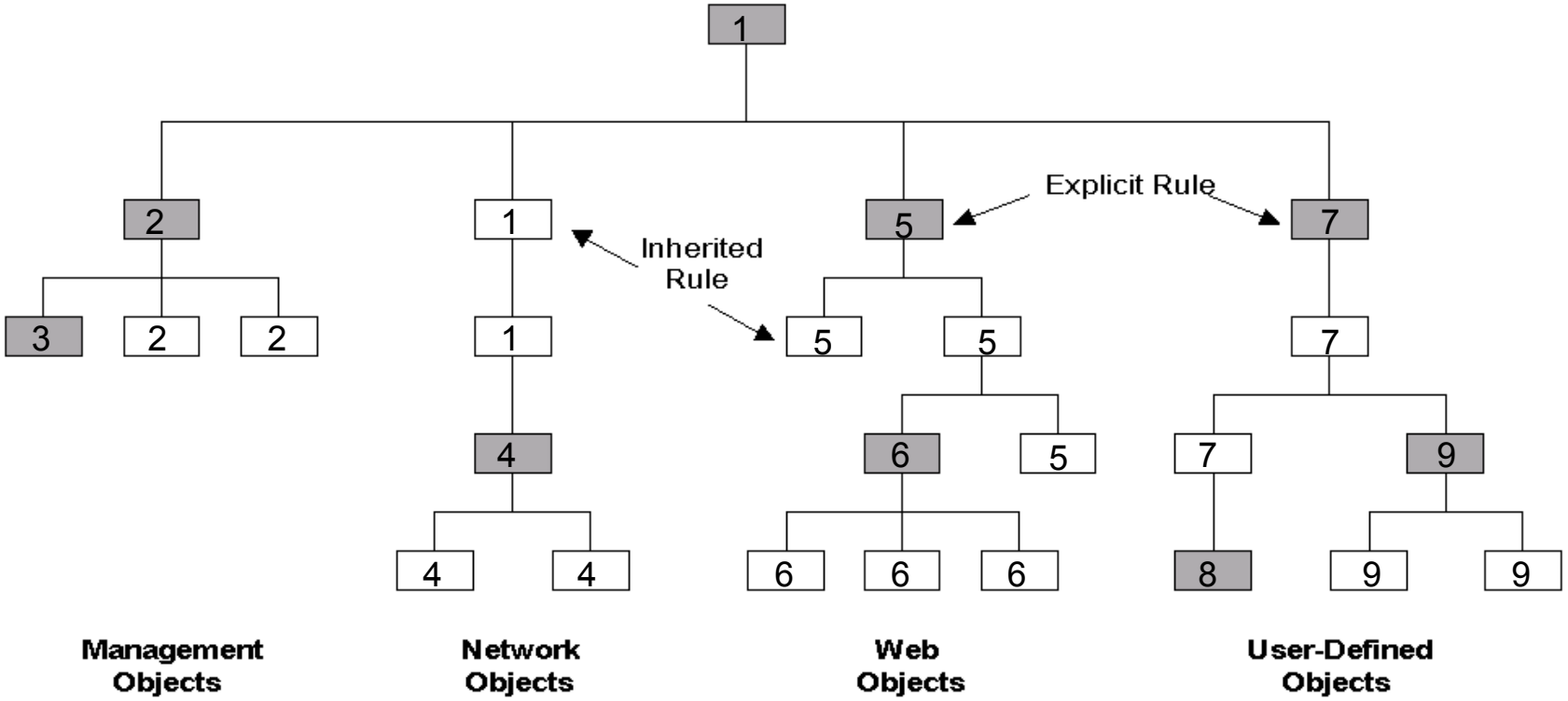
Input:

- Identidad
- Objeto accedido
- Acción

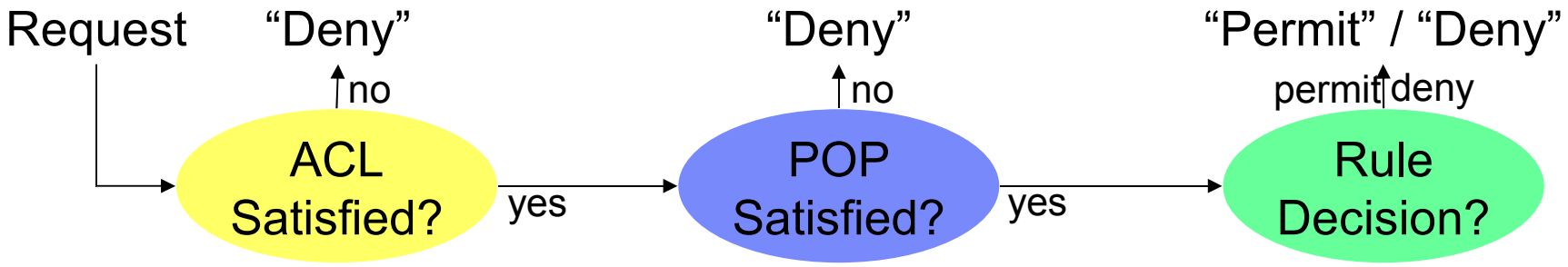
Resultado:

- Permitido
- No permitido

Modelo de autorización.
Espacio de Objetos Protegidos



Autorización. Tipos de control



Is Fred (in "Technical Sales" group) allowed to access specs?

Is the access request happening at an allowable time of day or day of the week?

Do one or more dynamic variables satisfy an established rule?

EJEMPLO:

- Permitir solo a los nuevos clientes
- Permitir solo a clientes con límite de crédito > 10,000 €

IF fecha alta > 10/10/2005
THEN Permit Access

IF credit limit > $10,000
THEN Permit Access

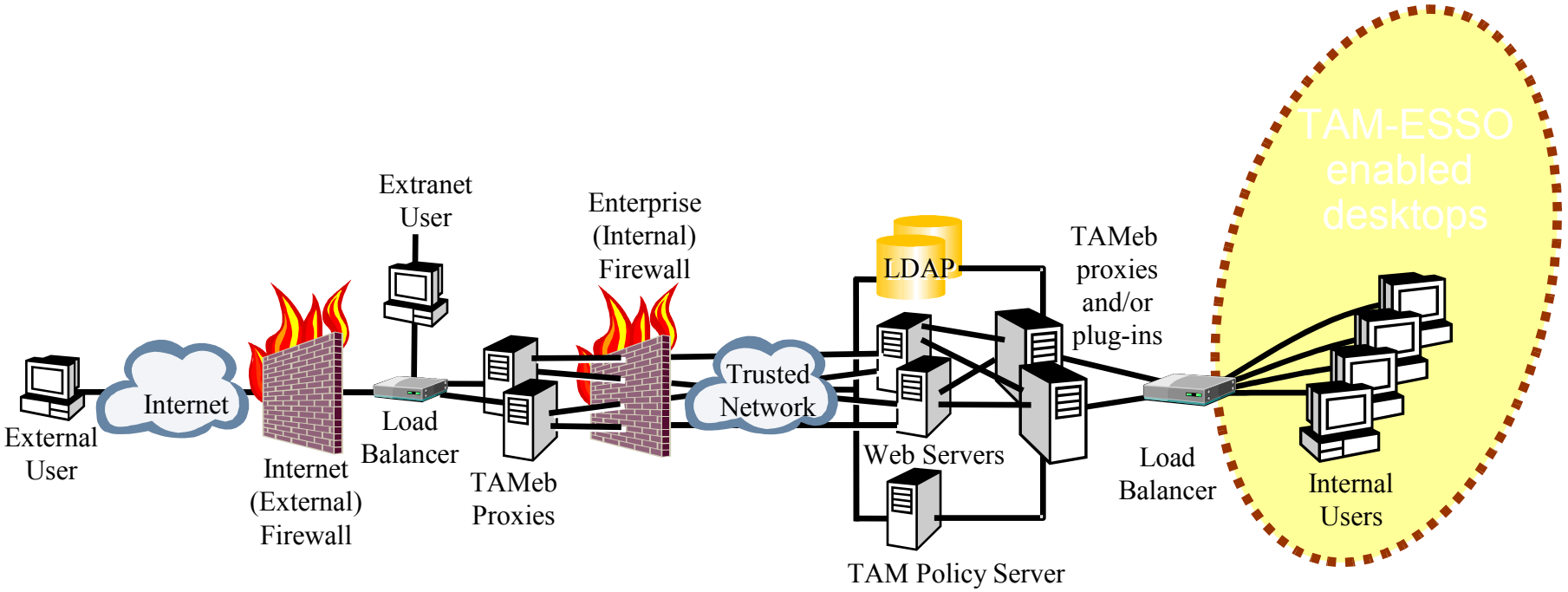
attach

attach

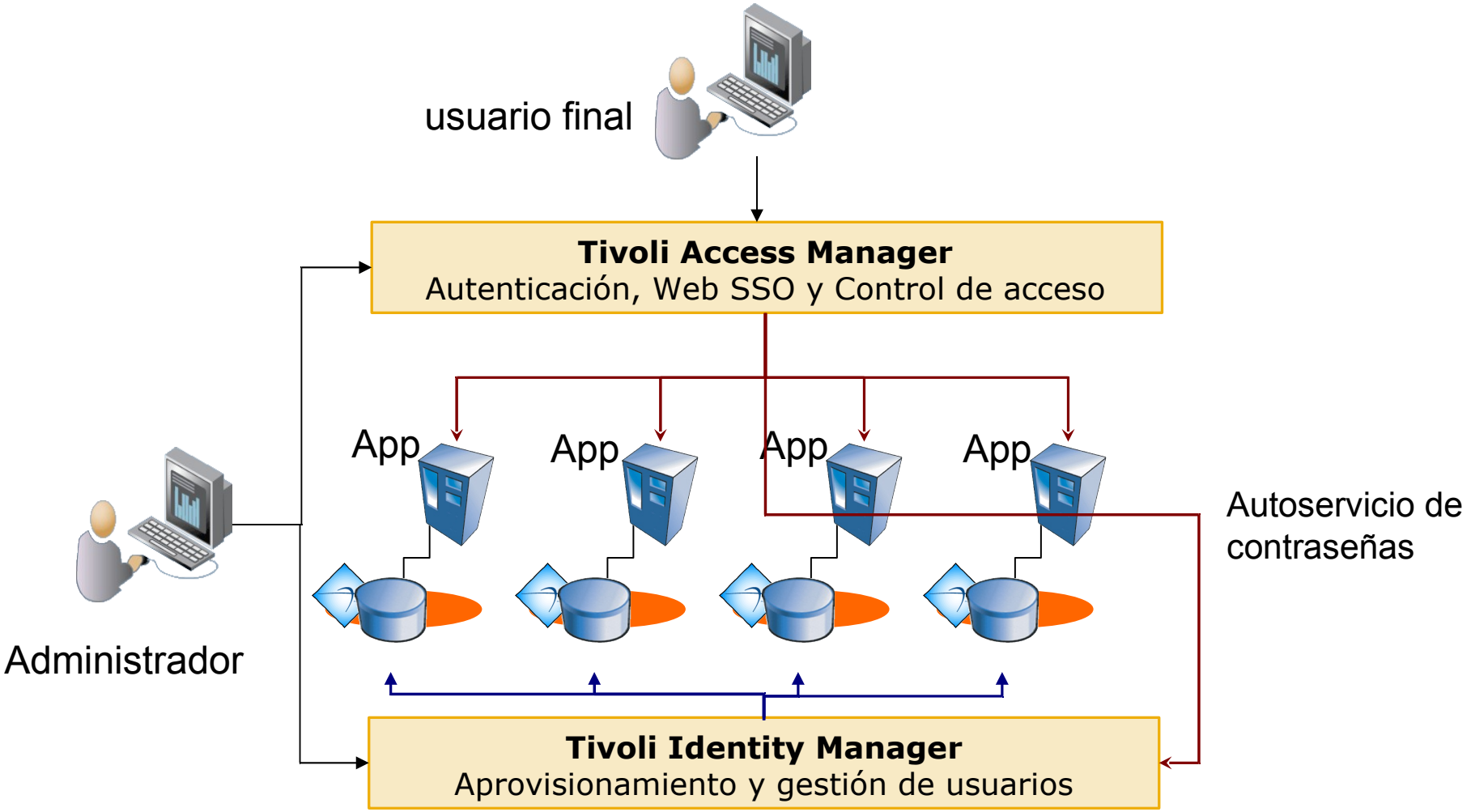
Protected Objects

TAMeb & TAM-ESSO

- **TAMeB (Internet, extranet, intranet)**
  SSO, autenticación y administración centralizada del control de acceso a Apps Web
- **TAM-ESSO (Intranet)**
  SSO a todo tipo de aplicaciones, incluyendo TAMeB
- **TAMeb and TAM-ESSO utilizan el mismo directorio de usuarios**

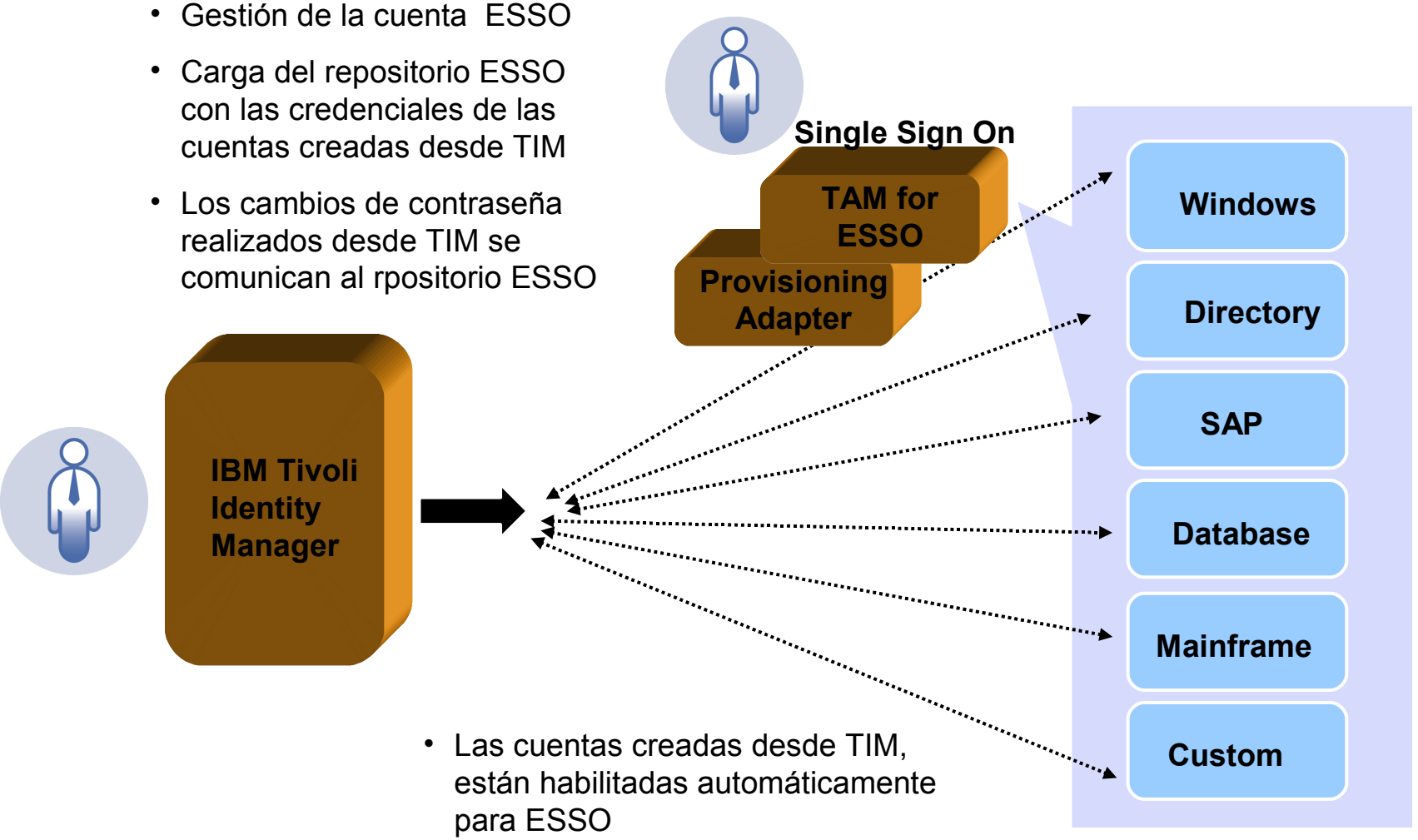


Integración TAMeB - TIM



TIM & TAM-ESSO

- Gestión de la cuenta ESSO
- Carga del repositorio ESSO con las credenciales de las cuentas creadas desde TIM
- Los cambios de contraseña realizados desde TIM se comunican al rpositorio ESSO



- Las cuentas creadas desde TIM, están habilitadas automáticamente para ESSO

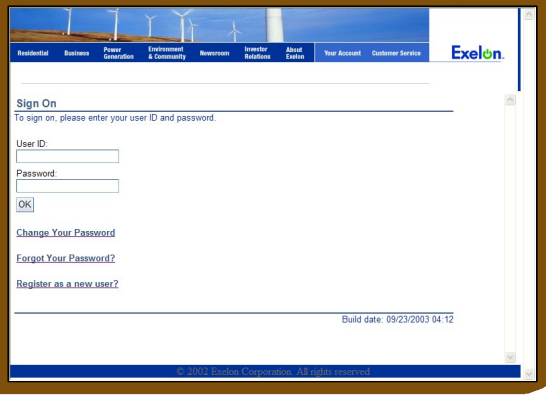
TIM permite el reset de la contraseña primaria de ESSO, o de cualquier otra contraseña gestionada

- Reset de contraseña de TAM-ESSO

TAM for ESSO & the Desktop Password Reset Adapter

- Through TAM for ESSO, Desktop PW Reset allows password reset directly from locked workstation

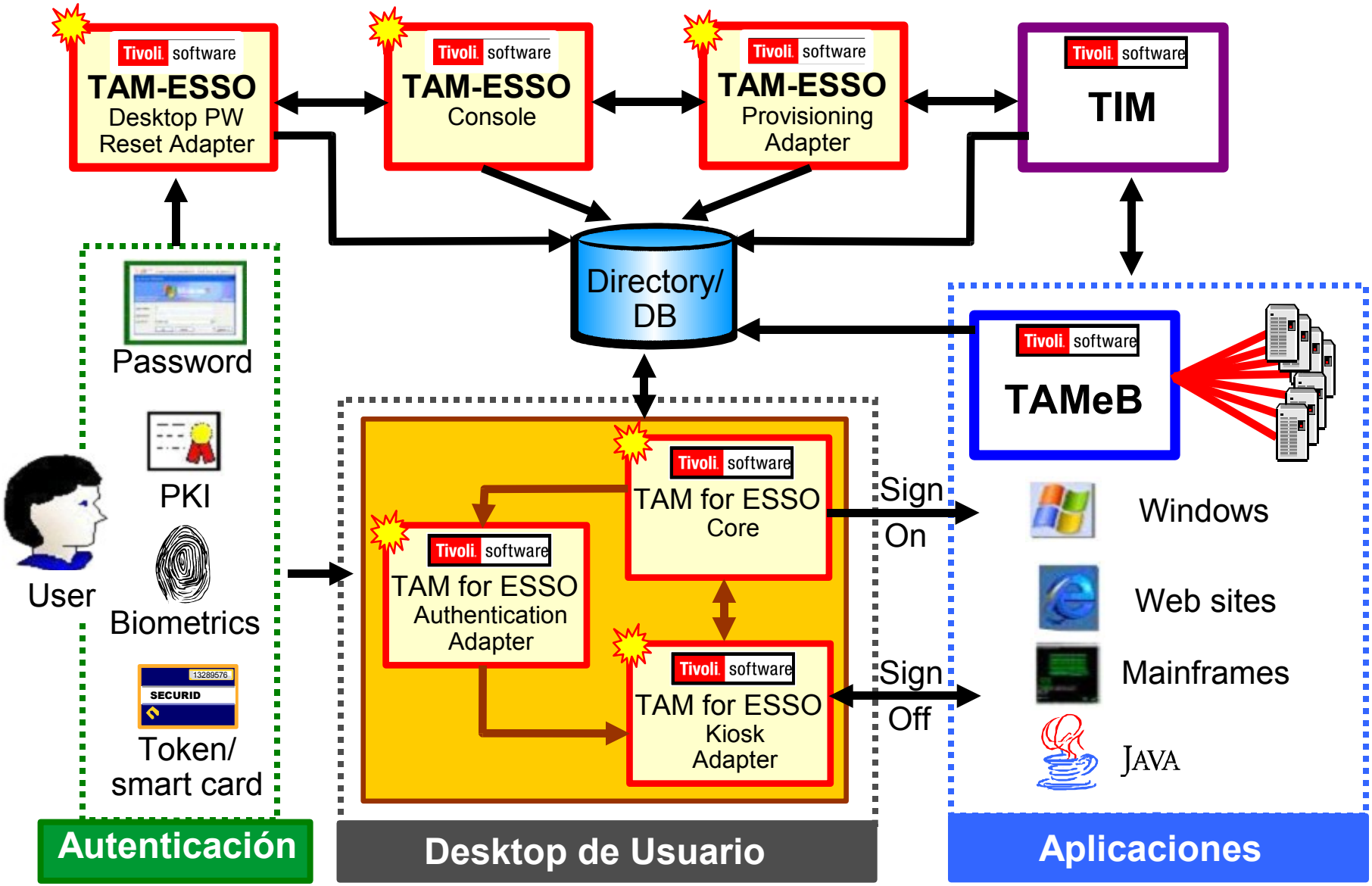
IBM Tivoli Identity Manager



- Reset de contraseña de cualquier sistema gestionado

- Windows
- Directory
- SAP
- Database
- Mainframe
- Custom

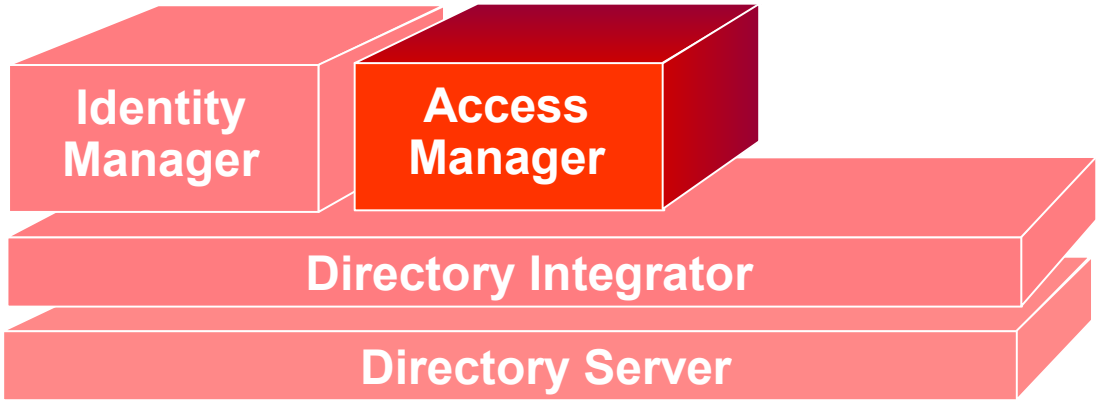
Integración TAM-ESSO,TAMeB y TIM



= Powered by passlogix

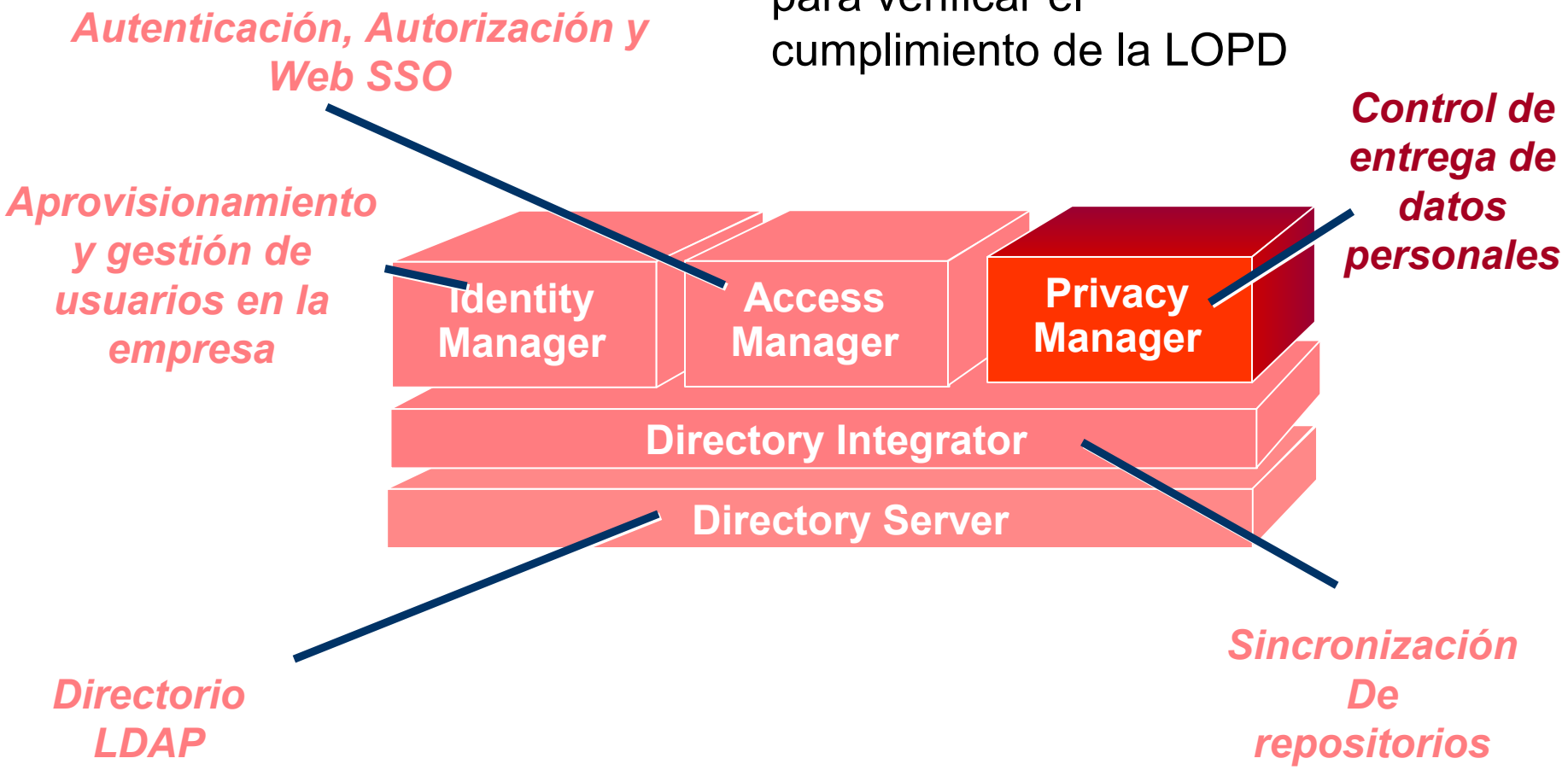
Familia Tivoli Access Manager

SSO PARA TODO TIPO DE APLICACIONES
ADMINISTRACIÓN CENTRALIZADA DEL CONTROL DE ACCESO PARA APLICACIONES WEB
AUTENTICACIÓN FUERTE
TOTALMENTE INTEGRADO CON TIVOLI IDENTITY MANAGER



ITPM – IBM Tivoli Privacy Manager

La infraestructura necesaria para verificar el cumplimiento de la LOPD

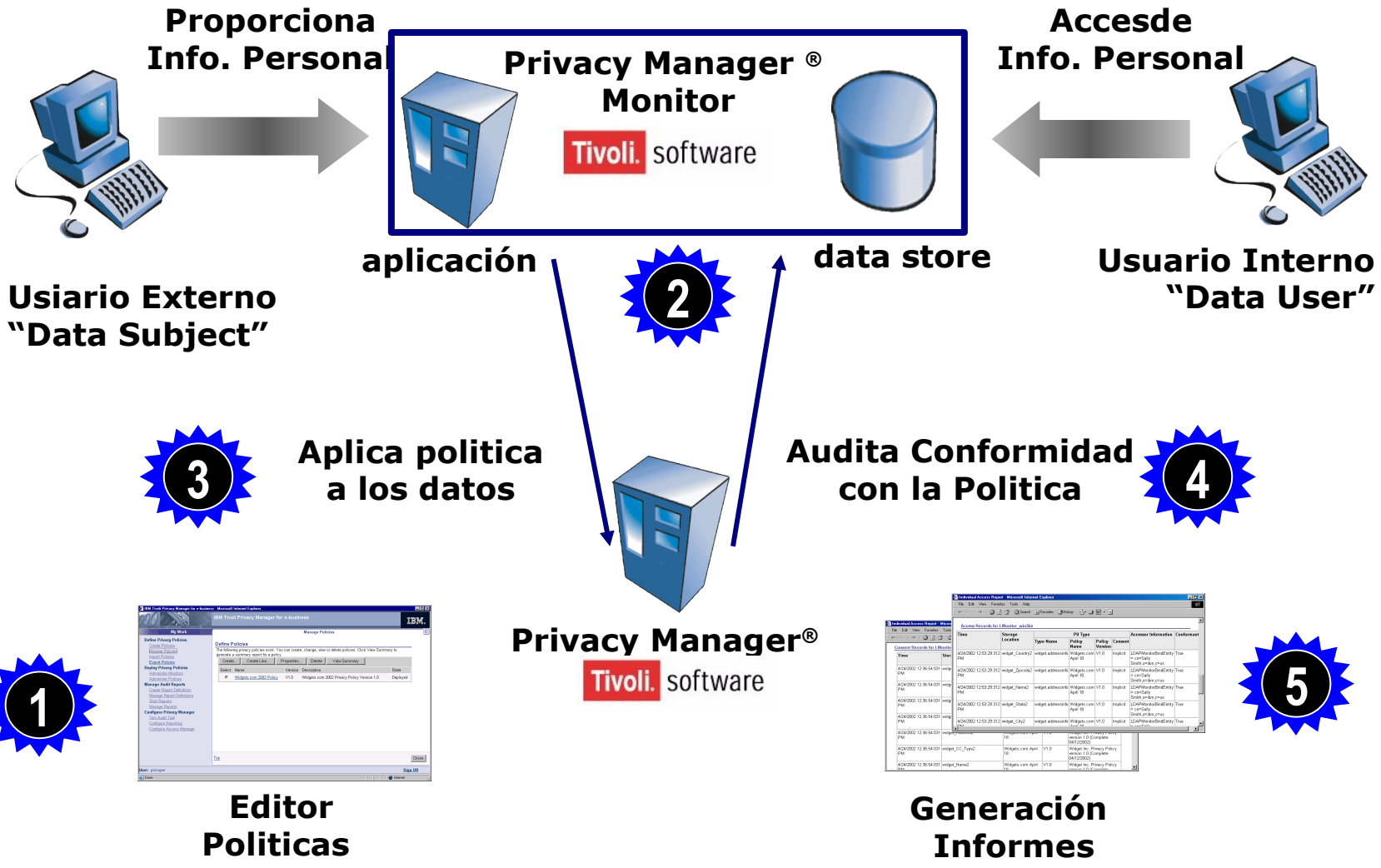


Que distingue a Tivoli Privacy Manager?

Controles de entrega	Controles de Acceso
▪ Que datos quieres utilizar? ▪ Con que propósito (App) ? ▪ Ha aceptado la persona registrada? ▪ Auditar: que datos se han entregado, a quien, para que	▪ Quien eres? ▪ A que grupos perteneces? ▪ Estas autorizado a acceder a este recurso ▪ Auditar: login, quien y cuando

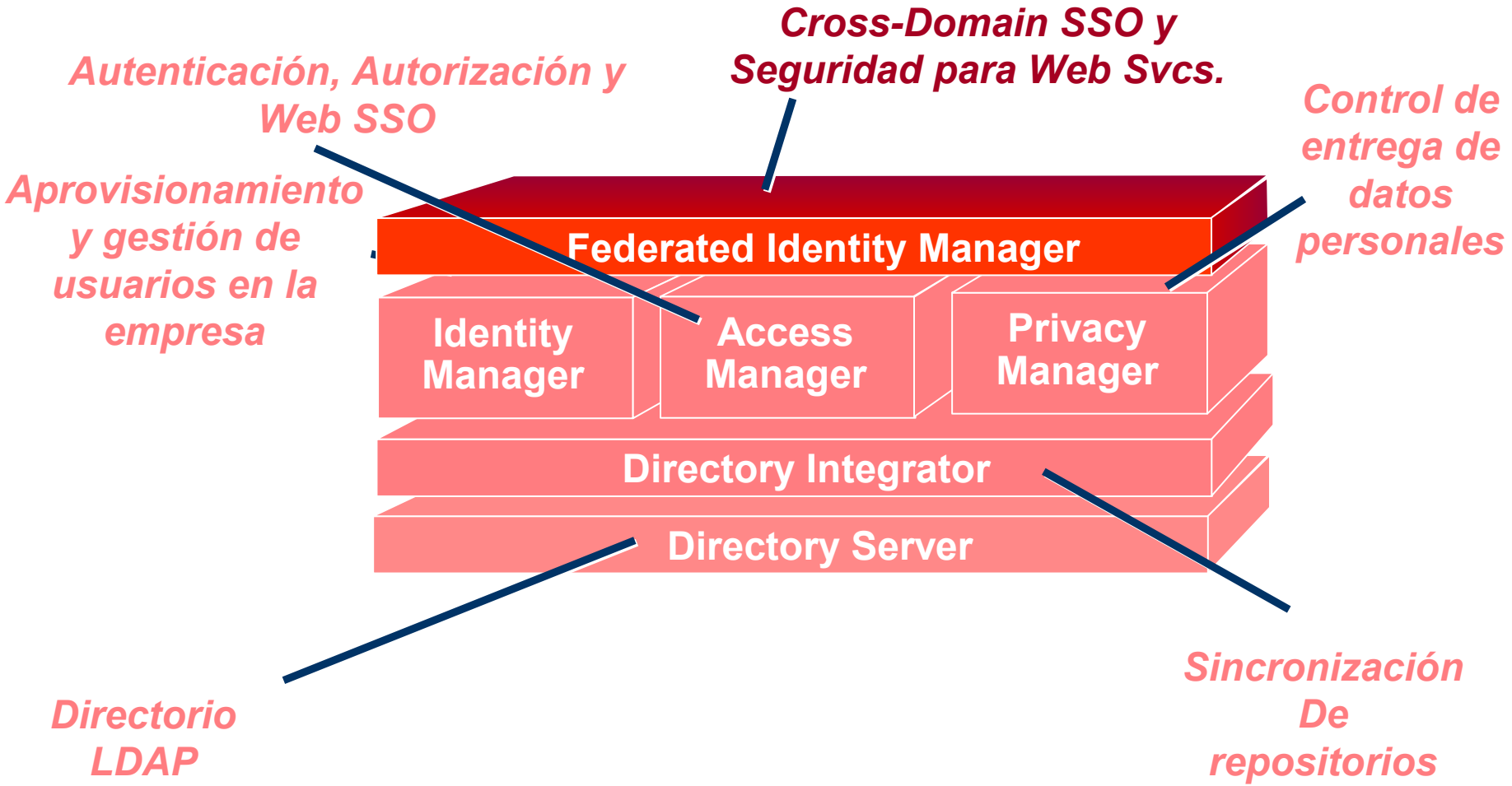
- Control de entrega
  - El usuario puede estar autorizado a acceder a una aplicación, pero puede no estarlo a acceder a ciertos datos.
  - Se pueden aplicar políticas antes de que los datos sean entregados a la aplicación
  - Es posible auditar el “path de entrega de los datos”

Que Hace Tivoli Privacy Manager?



Tivoli Federated Identity Manager

La solución para la gestión completa del ciclo de vida de usuarios en el seno de una federación



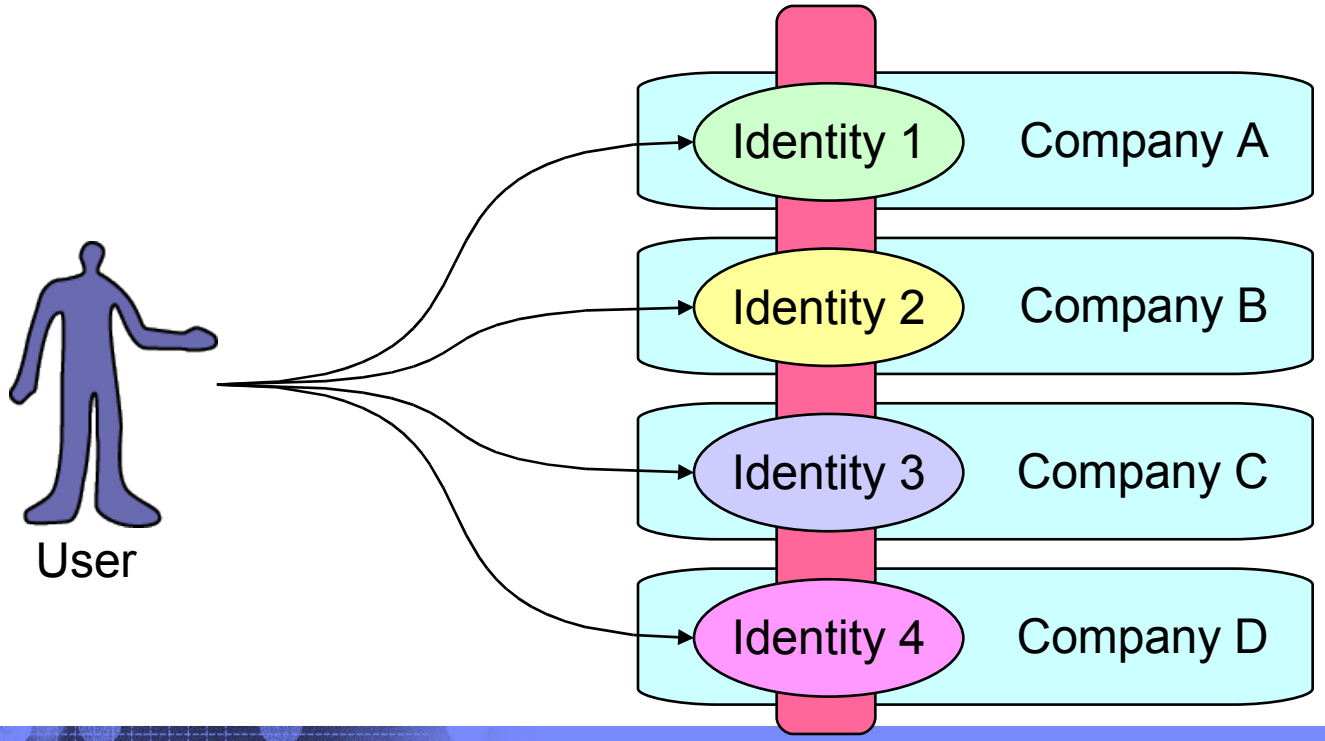
Problemática -> Interoperabilidad, gestión de identidades y logón único a recursos de distintos propietarios

1. No hay mecanismos standard para establecer relaciones de confianza con terceros
2. Esa carencia implica la replicación de la información de usuarios/cuentas
3. Gestión ineficiente y costosa de las identidades
4. Problemas de seguridad y privacidad -> inhibidores del negocio

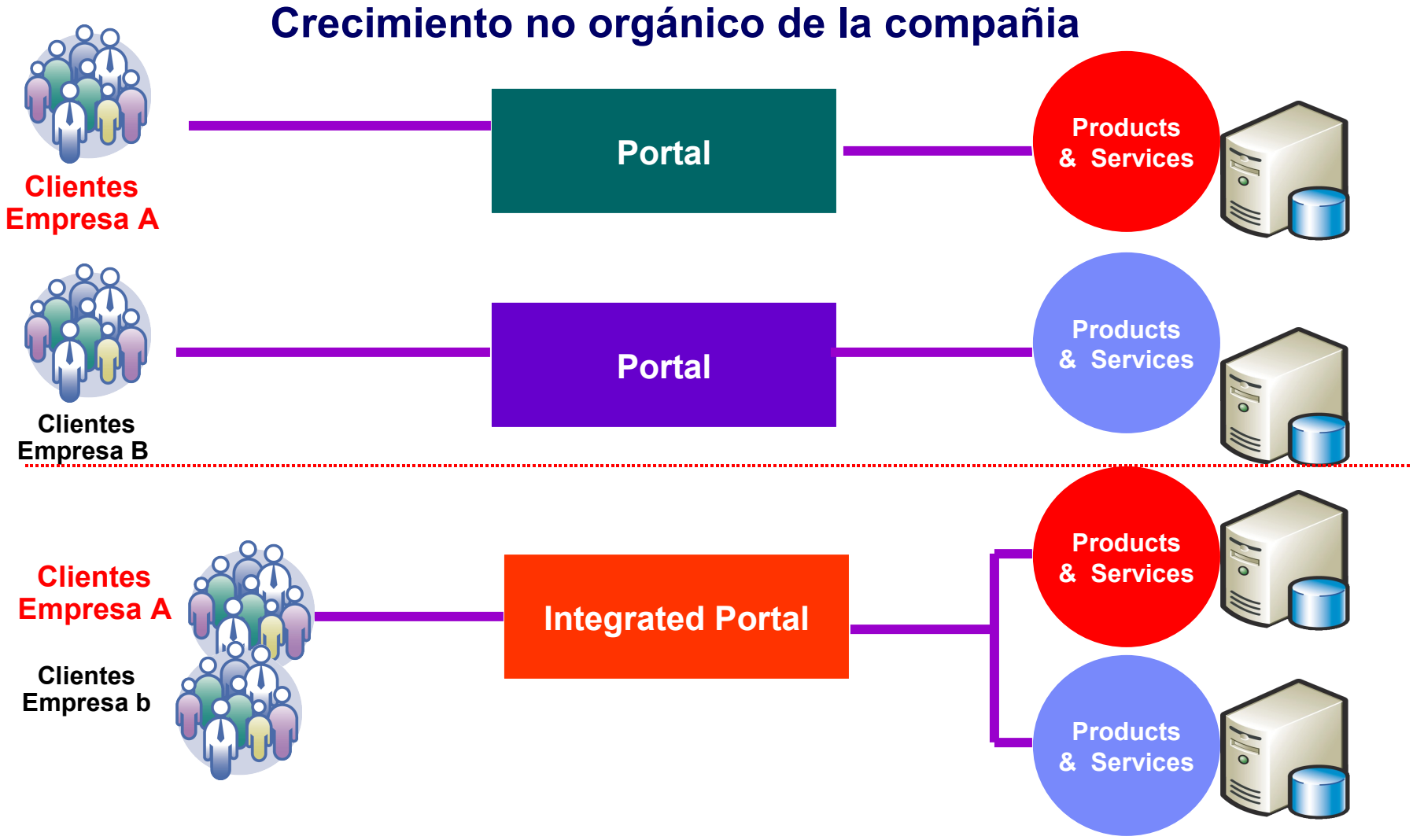
Solución => Federación de identidades

- ***Un conjunto de acuerdos tecnológicos y de negocio que permitirán que un usuario de una de las partes participantes en la federación pueda acceder a recursos de otro de los participantes de forma transparente, en un entorno seguro y de confianza***

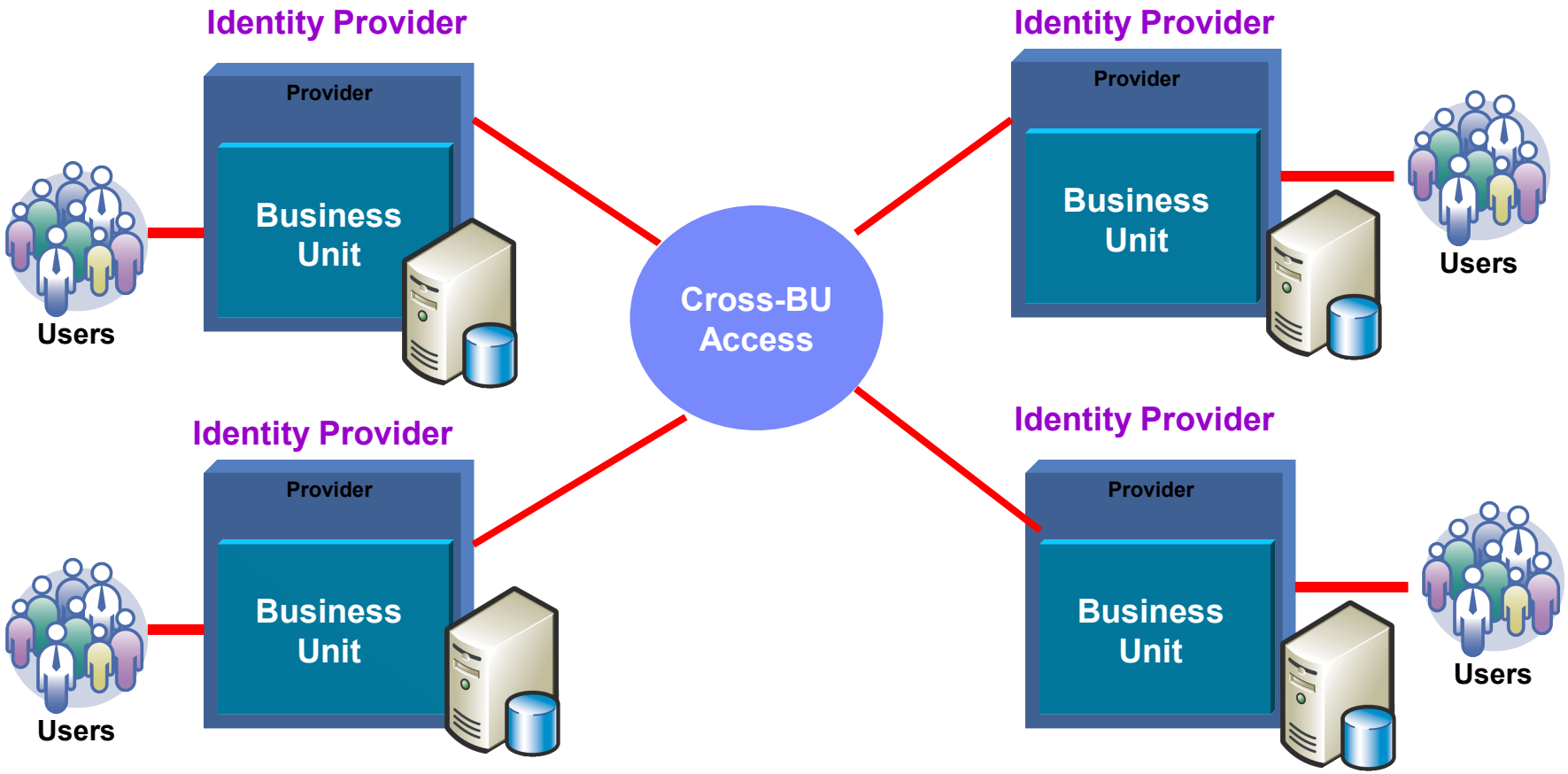
- ***El proceso de relacionar distintas identidades, gestionadas por entidades independientes, en general, con un único usuario final***



Escenarios de aplicación: Fusiones, Adquisiciones, etc

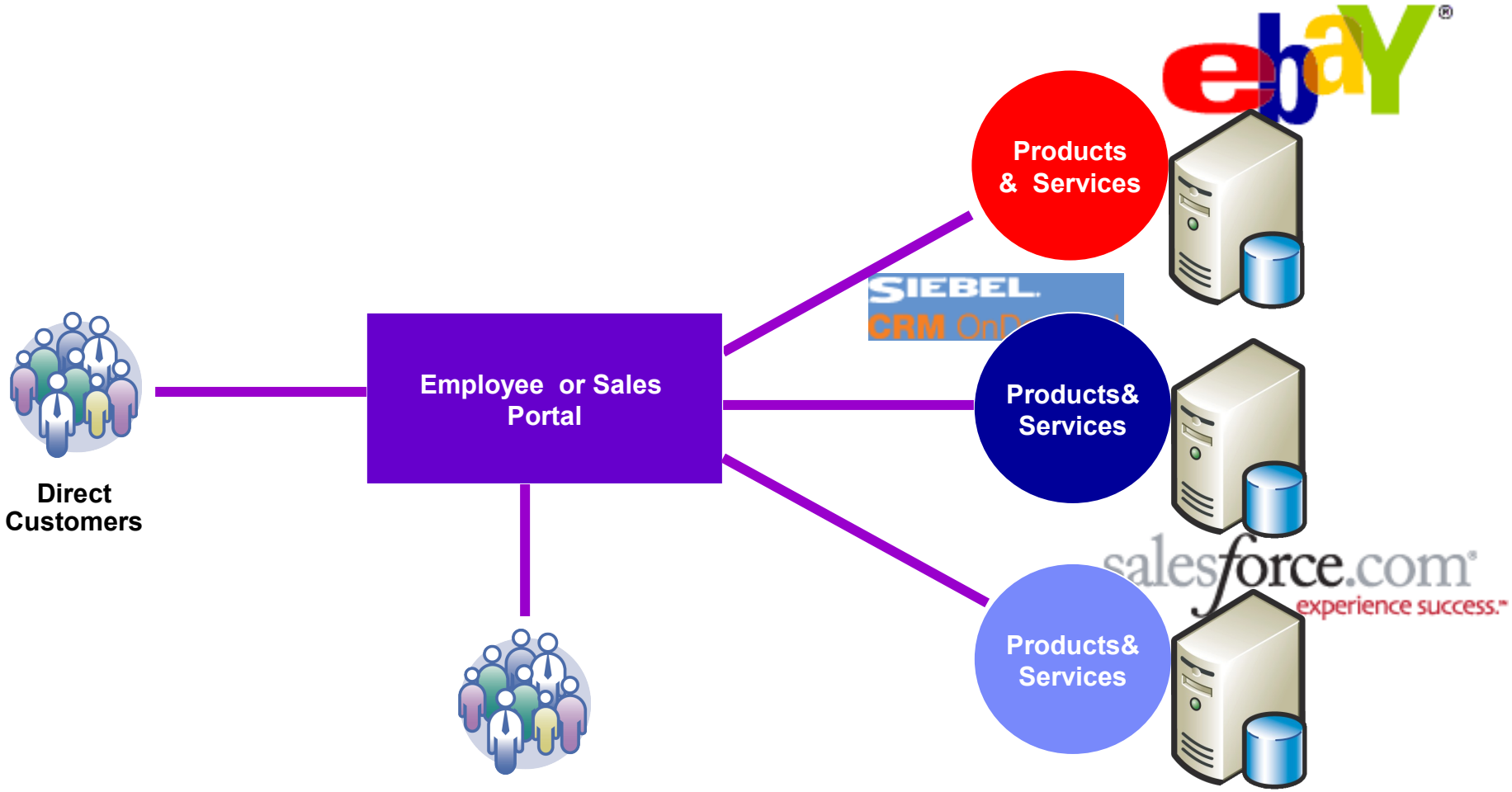


Escenarios de Aplicación: Interoperabilidad entre unidades de negocio independientes



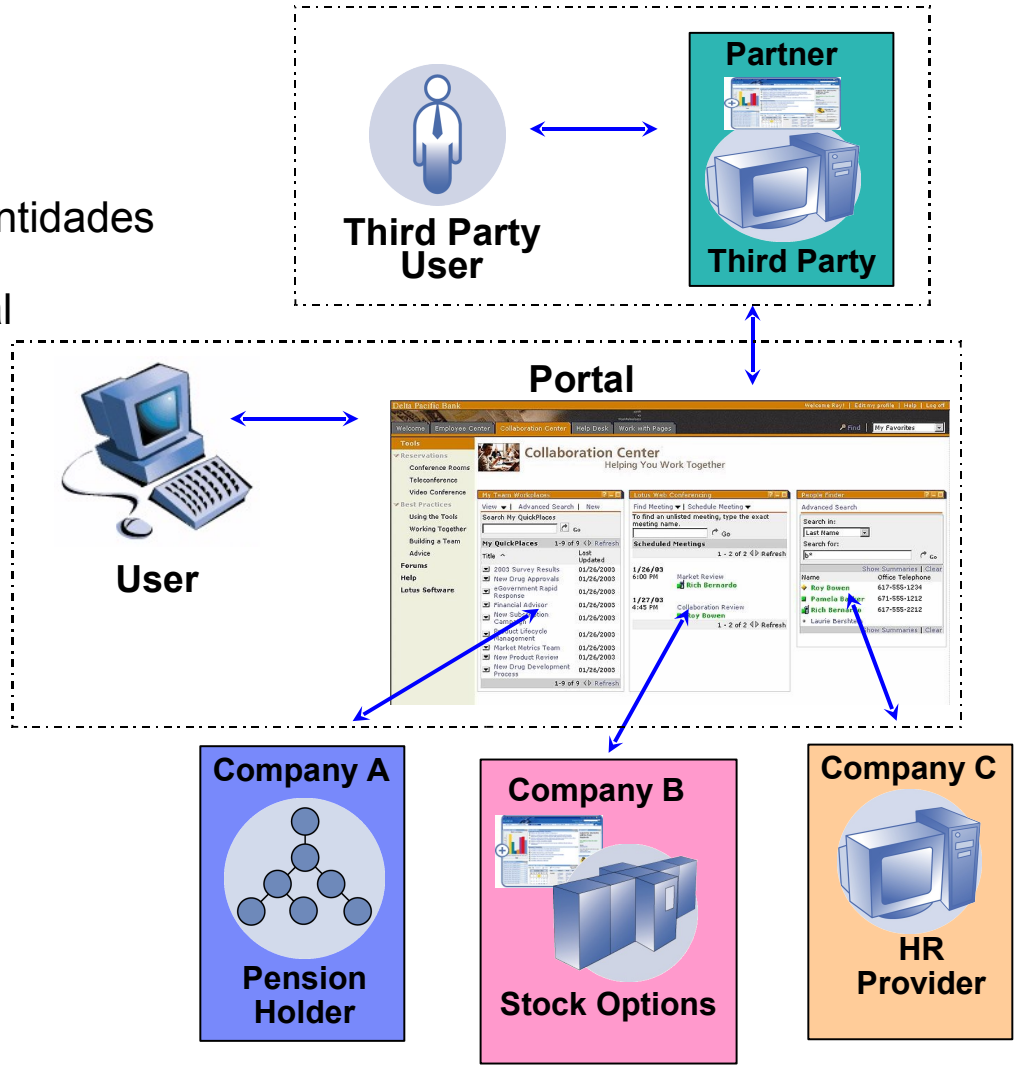
Federation de identidades para acceso a recursos distribuidos por las distintas unidades de negocio

Escenarios de Aplicación: Portales de negocio, SSO a/para/entre Socios y Proveedores, Portales del empleado con acceso a recursos prestados por Terceros



Propuesta de Valor de la Federación de Identidades

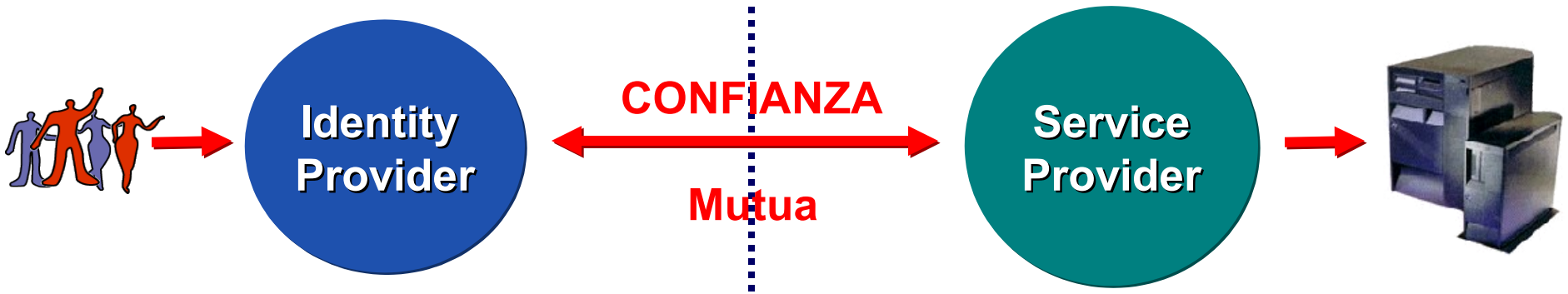
- Simplifica el proceso de integración
- Reduce de los costes de Gestión de Identidades
- Mejora de la experiencia del usuario final
- Proporciona Control y auditabilidad
- Crecimiento nº clientes potenciales
- Facilitador del negocio en red: seguridad, **privacidad**



Roles en la Federación: Identity Provider y Service Provider

Parte "garantizadora" en la transacción

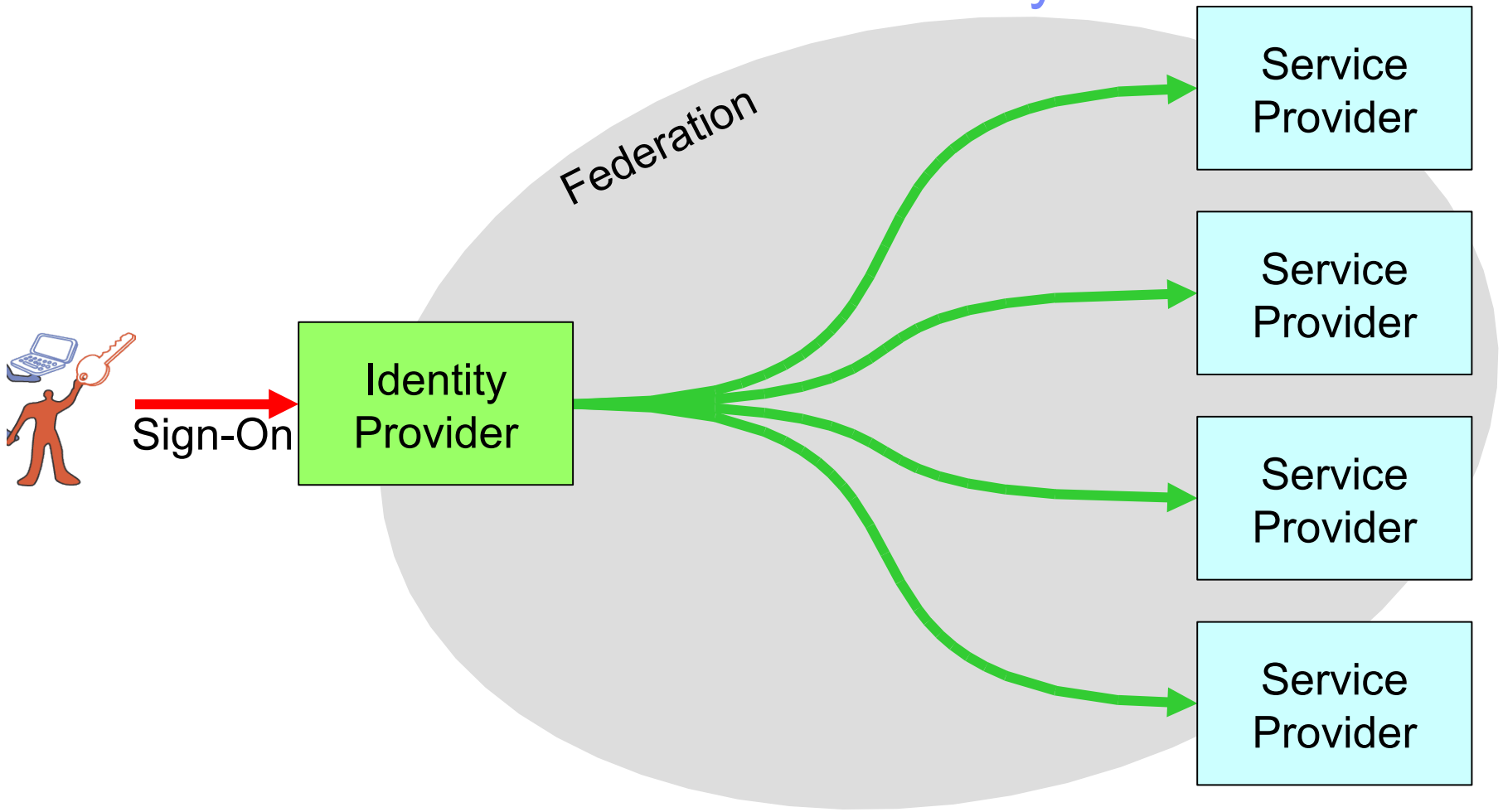
Parte "que valida" en la transacción



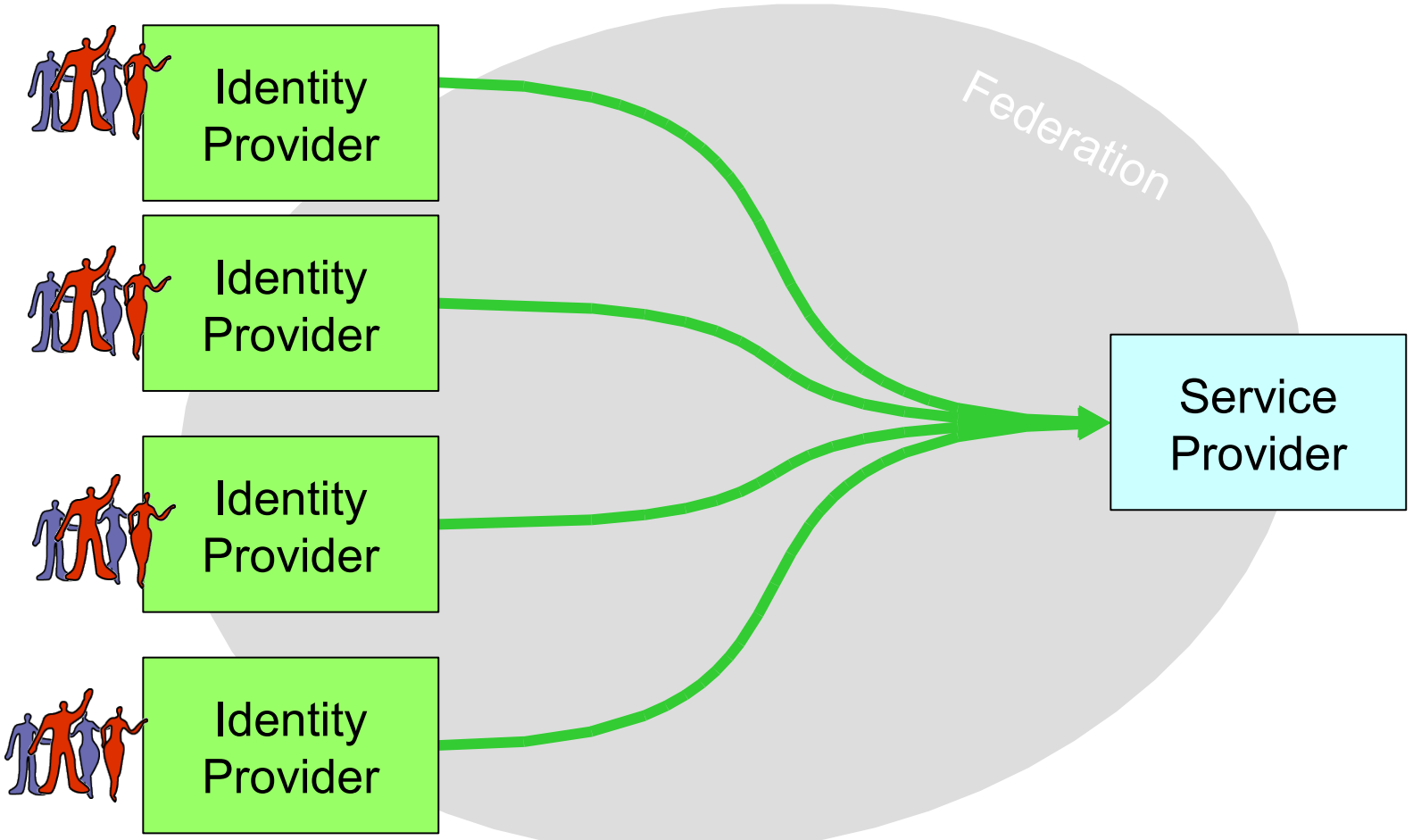
1. Proporciona credenciales en la Red/Login.
2. Gestiona la administración de IDs de Usuario
3. Autentica al usuario
4. "Garantiza" la identidad del usuario

1. Controla el acceso a los Servicios
2. El usuario tiene acceso a los servicios durante el período de duración de la federación
3. Solo gestiona atributos del usuario relevantes al SP

Vista de la federación desde el Identity Provider



Vista de la federación desde el Service Provider



Funcionalidad a alto nivel de TFIM

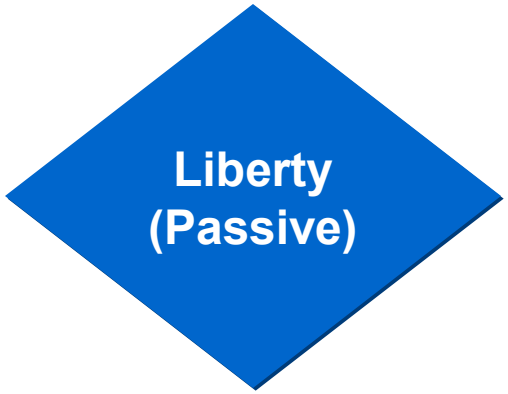
- **Permite desempeñar los roles de Proveedor de Identidades y Proveedor de Servicios en el seno de una Federación y proporciona la Gestión del Ciclo de vida del "Usuario Federado"**
  - Single Sign On, Single Sign Off, Account Linking, Account De-linking, Identity Provider determination (WAYF)
- **Proporciona funciones de Gestión de la Seguridad para Web Services**
  - Authenticación y Autorización de las peticiones a Web Services
- **Proporciona funciones de Gestión del aprovisionamiento de Ususarios Federados**
  - Aprovisionamiento de usuarios y datos de usuarios (atributos, suscripciones …) ENTRE MIEMBROS DE LA FEDERACIÓN

TFIM Soporta los tres estándares del mercado

HTTP SSO (SAML protocol)

- Single Sign On

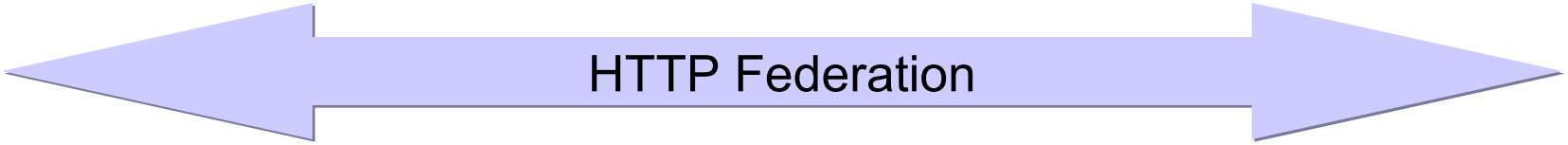
Identity Federation Mgt (SAML protocol)



- Single Sign On
- Single Sign Off
- Account Linking, De-Linking
- Identity Provider Determination

ID Management para Federated Web Services (HTTP and SOAP-based SSO)

- Single Sign On/Off
- Identity Provider Determination



Gestión del Cliclo de vida del Usuario Federado, algo más que Single Sign On

- **Single Sign On es solo una parte de la gestión del ciclo de vida**

- **TFIM tambien proporciona**

  Single Logout

  Elimina las sesiones de SSO establecidas en la federación

  Identity Provider Determination

  Soporta Protocolos “Pull” – permite que el SP “encuentre” el IDP del usuario

  Account Linking (empleando Alias)

  Proporciona a las dos partes una forma común de referirse a un usuario

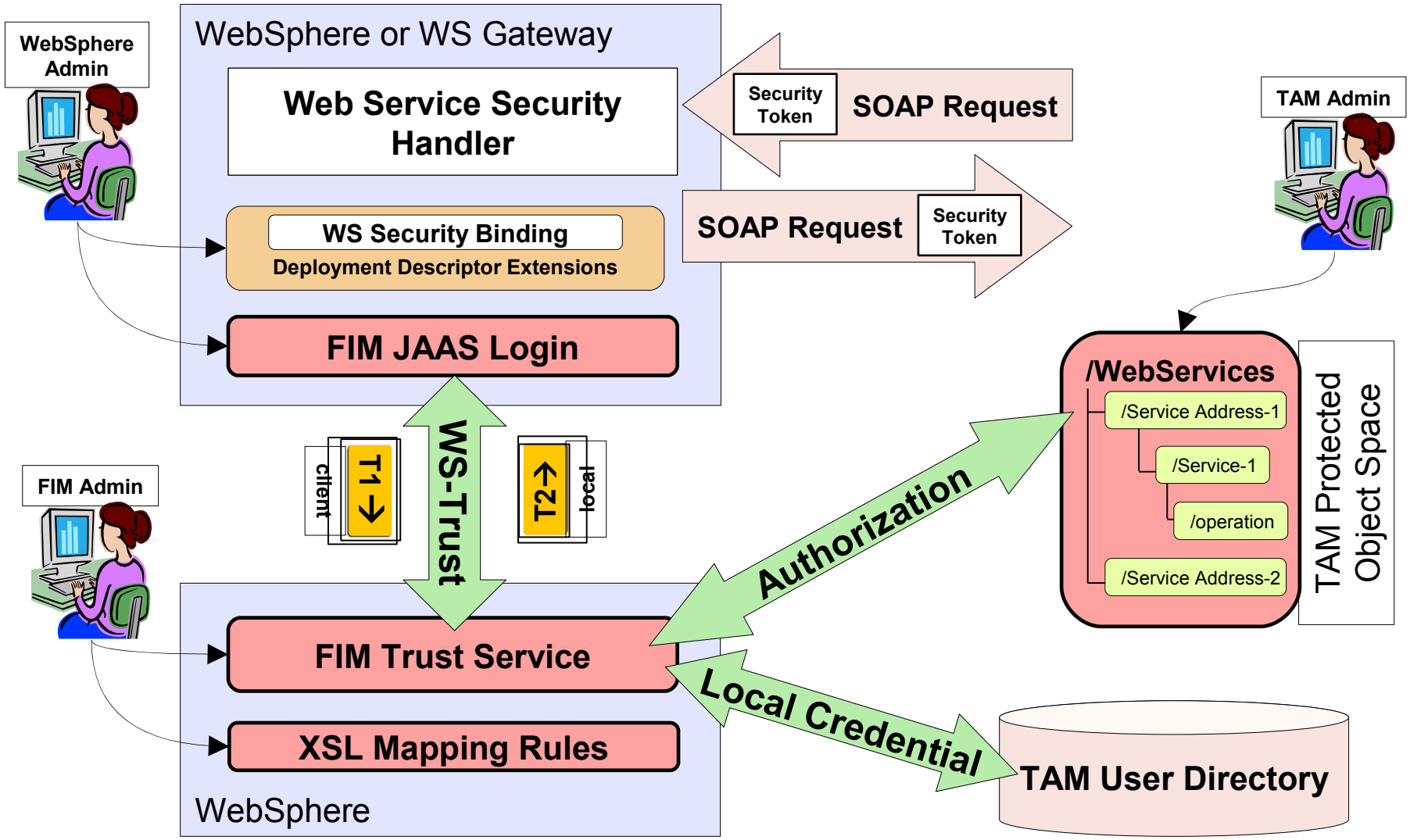
  Habilita Single Sign On con privacidad

  Account DeLinking

  Deshabilita el SSO

  Sin una referencia común de usuarios, no es posible realizar SSO

TFIM Web Services Security Management



Gestión de Seguridad en Web Services

- **Gestión de Tokens**

  Validación de tokens (soporte de múltiples formatos de token)

  Identificación del cliente web service especificado en el Security Token

- **Mapeo de Identidades**

  Asocia la identidad remota (en el token) a una identidad local (servidor)

  Obtiene credenciales para la identidad local.

- **Gestión de Autorización**

  Aplica políticas de control de acceso a la petición Web Services.

  Decisión de autorización basada en las credenciales locales

Aprovisionamiento Federado

Aprovisionamiento

Aprovisionamiento Federado

Aprovisionamiento Local

Proveedores de servicios

Portal Empleado

Suministrador

Socios

Desde el punto de vista de negocio TFIM…

- **Facilita una "Arquitectura Orientada al Servicio"**
  - Permite ofrecer servicios, de forma segura a todos los usuarios de la federación
  - Mejora la experiencia de usuario proporcionando Logón Unico,
- **Rebaja los costes de Gestión de Identidades**
  - Solo los "Identity Providers" gestionan información de autenticación
  - Los "Service Providers" gestionan solo información relevante a su servicio
- **Proporciona Automatización de las funciones de Aprovisionamiento entre compañias**
  - Aprovisionamiento de Identidades, atributos y servicios

Desde un punto de vista técnico TFIM…

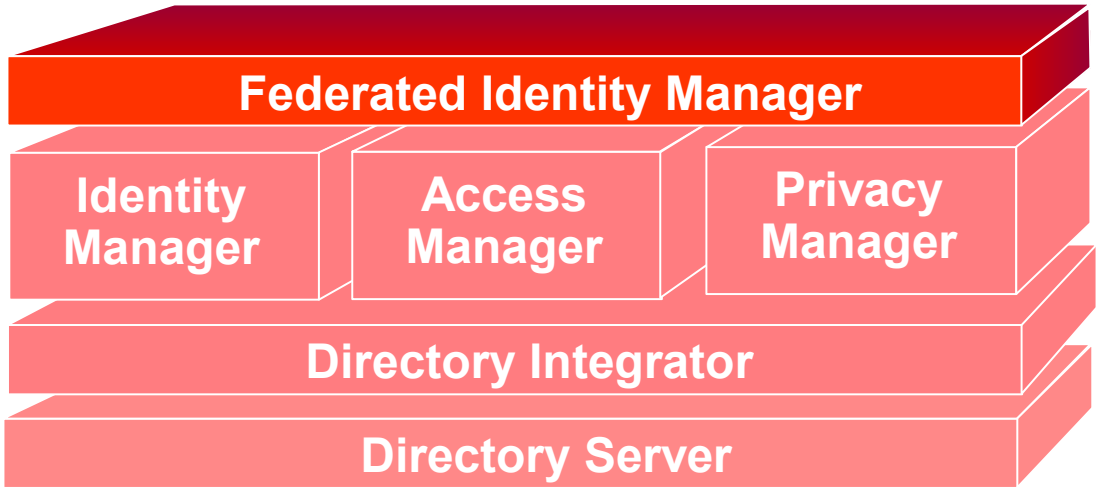
- **Simplifica la administración de identidades federadas (gestión del ciclo de vida) y proporciona funciones adicionales a la de Logón Unico: WSSM y WS-Provisioning**

- **Soporta múltiples standars y proporciona una gran interoperabilidad**

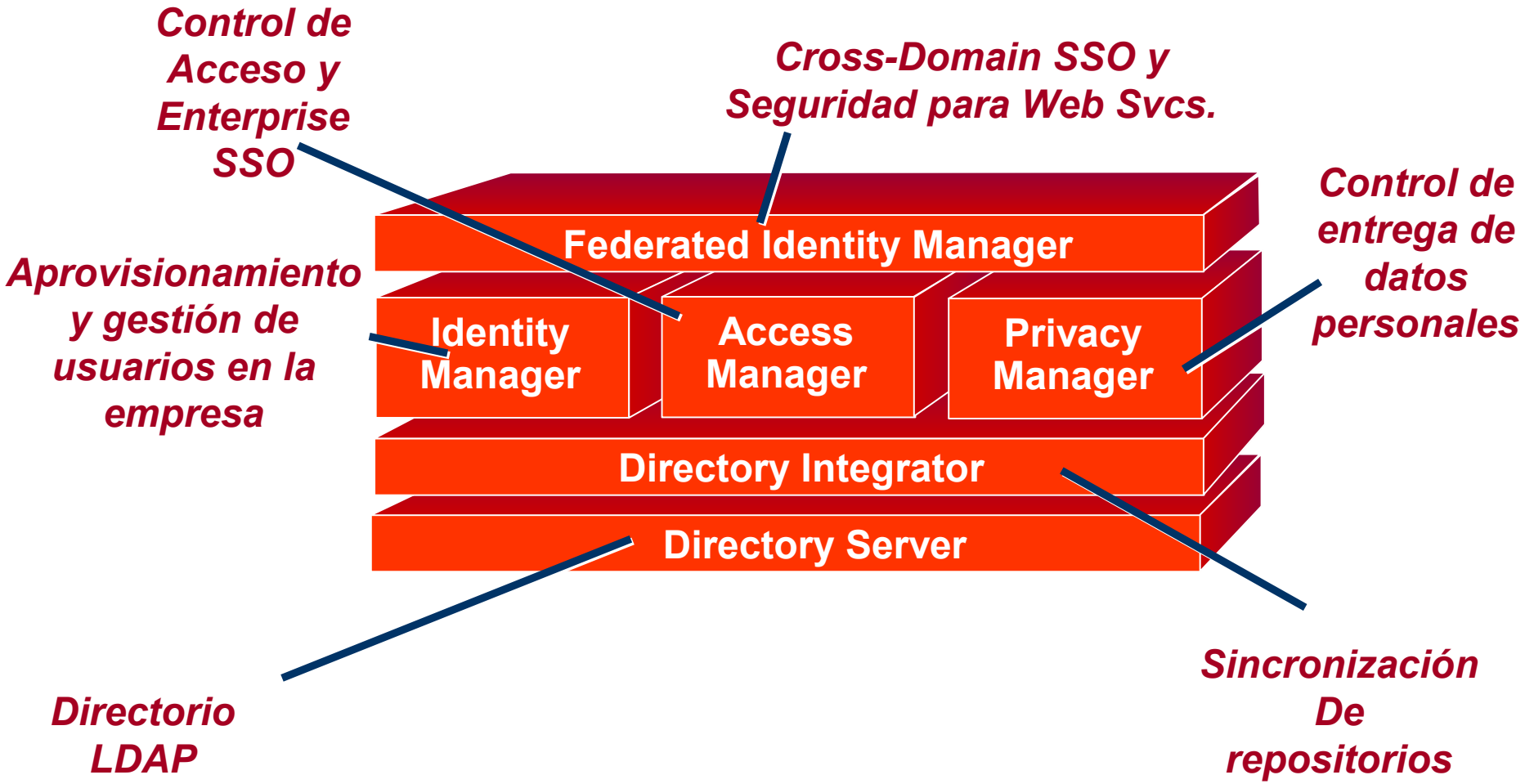
- **Está basado en productos y tecnologías IBM de probada solvencia en múliples instalaciones**

TIVOLI FEDERATED IDENTY MANAGER

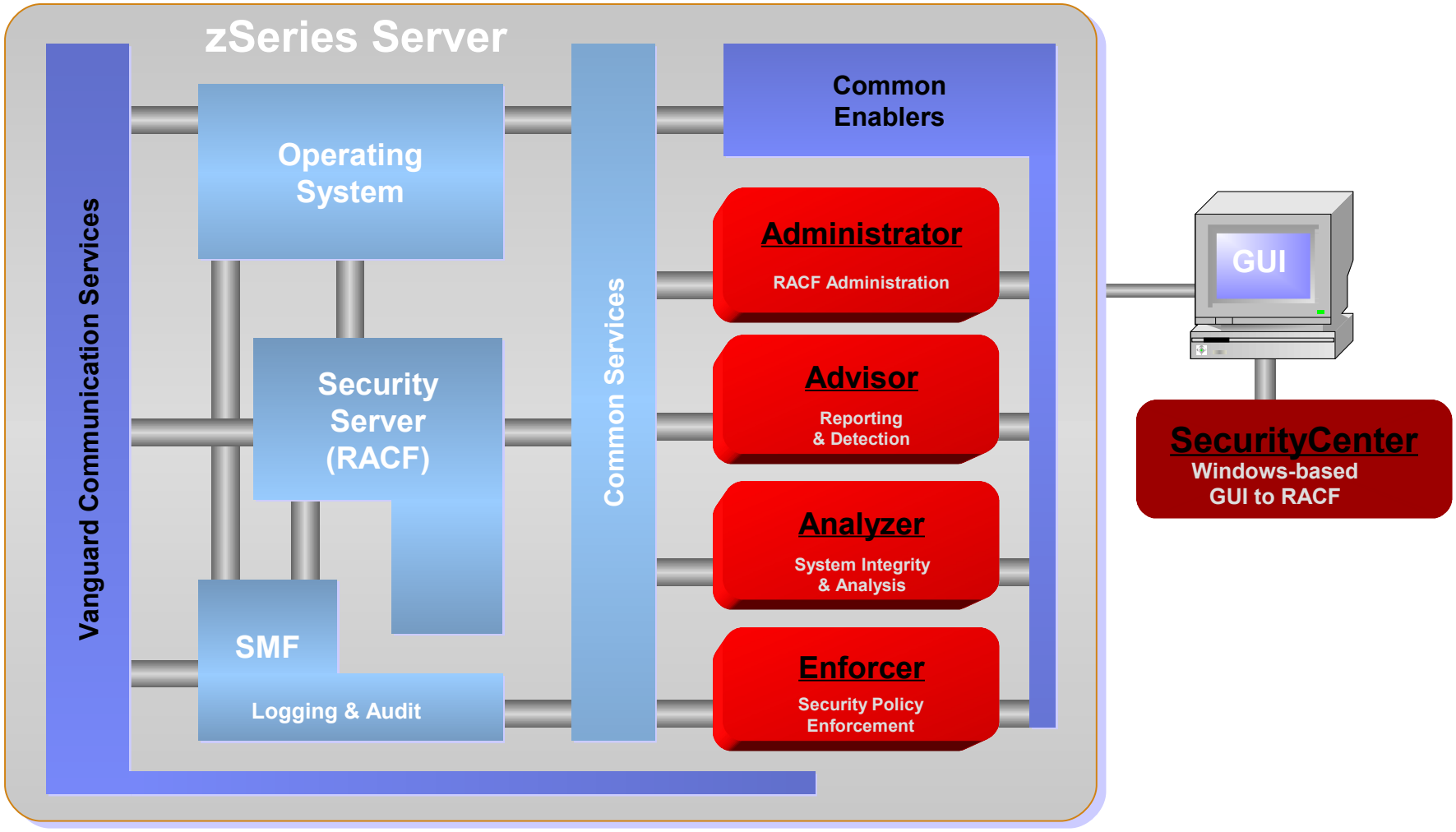
MUCHO MAS QUE SSO FEDERADO
SOPORTE DE MULTIPLES STANDARD
COMPONENTES TEGNOLOGICOS DE PROBADA SOLVENCIA



Catálogo Integrado de IBM para la gestión de identidades



VANGUARD SOFTWARE



Administración avanzada de RACF y Herramientas de Gestión de Políticas en z/OS

Vanguard Administrator

Herramientas de administration, data mining, reporting and analisis para RACF

Vanguard Advisor

Detección de eventos, analisis, generación de alertas en tiempo real y reporting

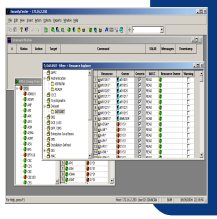
Vanguard Analyzer

Un sistema de asesoramieno, identificación de riegos y análisis de amenazas.

Vanguard Enforcer

Una solución de detección y gestión de intrusión en z/OS.

Vanguard SecurityCenter



Una interface windows interface al zSeries Security Server de IBM.

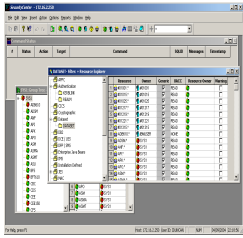
Vanguard Administrator – Simplifica la administración de RACF

Vanguard Advisor – Facilita la generación y distribución de Informes detallados , genera alertas en tiempo real

Vanguard Analyzer – Facilita la auditoria del z/OS, no solo de RACF

Vanguard Enforcer – Un gestor e impositor de políticas en tiempo real para el z/OS

Vanguard SecurityCenter – Un entorno gráfico mas amigable y facil de usar para el RACF



Preguntas .....