Gestión de Identidades y Accesos

Retos y oportunidades para grandes corporaciones

Philippe Reynaud, CISSP
Consultoría Banca y Seguros , Atos Origin

Índice

- Introducción
- Situación inicial y pasos previos
- Plataforma de gestión de Acceso
- Beneficios

Introducción

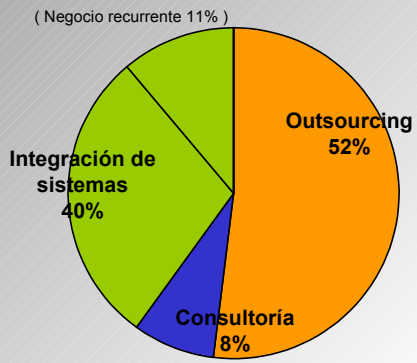
Introducción

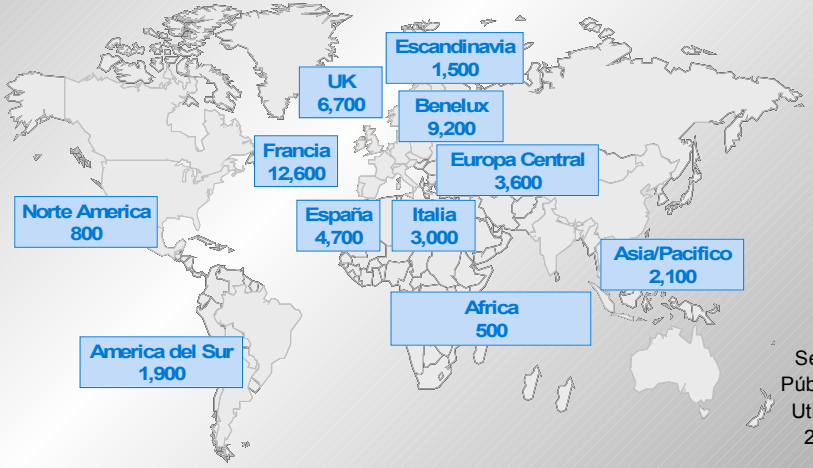
Quiénes somos

Líderes europeos en Tecnologías de la Información, ofreciendo **soluciones globales**

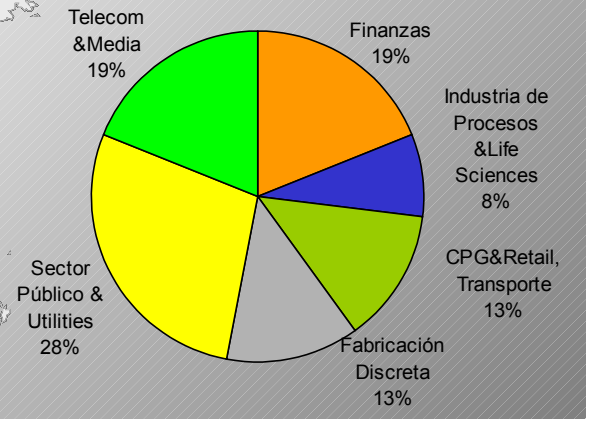
- ✓ **5.300 millones de euros de facturación**
- ✓ **46.000 empleados en 40 países**
- ✓ **2.500 consultores** ayudando a los clientes a transformar sus sistemas de negocio
- ✓ **12.000 especialistas** en Integración de Sistemas a nivel global
- ✓ **90 centros de proceso de datos** en todo el mundo
- ✓ **Atos Consulting** desde septiembre 2004
- ✓ **9 Software Factories** certificadas en CMM
- ✓ **Podium en los 6 países europeos** que conforman el 90% del gasto en IT

Desglose por prácticas





Desglose por sectores



Transformando en resultados la visión de nuestros clientes

Introducción

JJOO: Una oportunidad para hacerlo bien

Algunos datos de la magnitud del proyecto

- 35 disciplinas y 301 acontecimientos deportivos.
- 62 instalaciones.
  - Incluidas 36 para competiciones.
- 10.500 atletas.
- 21.500 representantes de medios de comunicación.
- Equipo de 3.500 profesionales de IT.
  - Incluidos voluntarios.
- Gestión de 60 aplicaciones.
  - +10.000.000 de líneas de código.
- 10.500 ordenadores.
- 900 servidores Intel y UNIX.
- 300 routers y 2,000 switches.
- 1 centro de disaster recovery.
- 200.000 acreditaciones.
- 4.000 terminales de sistemas para los resultados.
- 2.000 máquinas de fax y fotocopiadoras.
- 4.000 impresoras.
- 23.000 teléfonos.
- 1.500 terminales de información para periodistas.
- 2.500 terminales de intranet.
- Integración de 15 proveedores de tecnología.
- 200.000 alertas de seguridad diaras

The largest sports related Information Technology contract ever awarded

"We are extremely pleased to have expanded our partnership with Atos Origin as the Worldwide IT Partner for two more Games. Today the role and use of Information Technology is vital for the staging of the Games. Atos Origin had a crucial player in the success of the delivery of the ATHENS 2004 Olympic Games. We are confident that, in the future, Atos Origin will deliver an outstanding job for the Torino 2006, Beijing 2008, Vancouver 2010 and the 2012 Olympic Games"

Jacques Rogge, President of the International Olympic Committee.

Introducción

Los grandes retos del IAM

- Reducción de costes recurrentes en la administración de la seguridad
- Aprovisionamiento de usuarios
- … desaprovisionamiento de usuarios
- Evolución tecnológica, homogeneización
- Cumplimento estándares (Sarbanes Oxley)
- Multicanalidad
- Auditabilidad
- Capacidad de reacción
- Mantenibilidad de aplicaciones

Transformando en resultados la visión de nuestros clientes

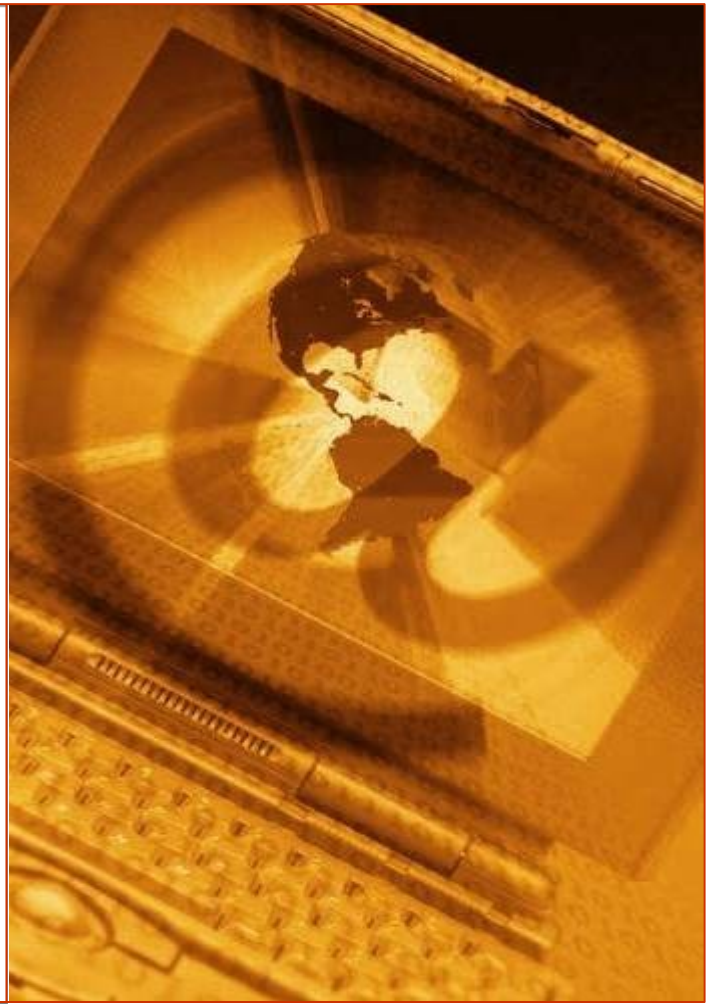
Enfoque clásico: complejidad IAM =
número de procesos de negocio * número de canales de distribución

Plataforma Multicanal orientada a servicios,
con gestión de identidades y accesos integrada

Introducción

Especificidad del sector financiero

- Número de canales de distribución
- Complejidad de los servicios ofrecidos
- Criticidad de los procesos de bastanteo
- Número y volumen transacciones
- Tamaño organización (empleados, colaboradores, clientes)
- Movilidad de usuarios
- etc…



Situación inicial y pasos previos

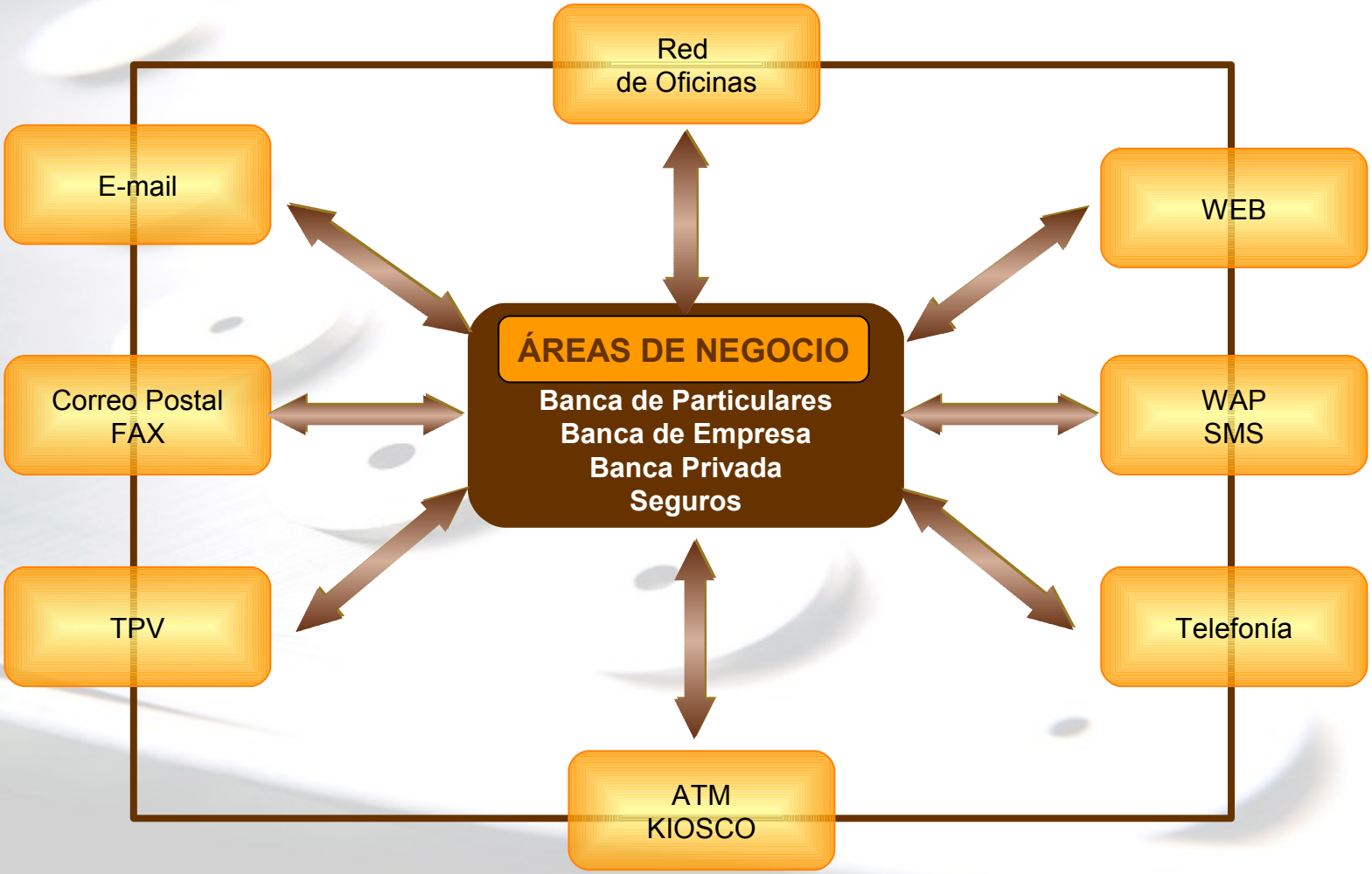
Situación inicial y pasos previos

Un caso de éxito …

- **Cliente de Atos Origin España**
- **Sector financiero**
- **Tamaño medio**
- **Alto nivel tecnológico**

Situación inicial y pasos previos

Canales de distribución



Transformando en resultados la visión de nuestros clientes

Situación inicial y pasos previos

Gestión, control y servicios

Gestión de los accesos

- Segmentación procesos
- Perfilado aplicativos
- Habilitaciones

Gestión del ciclo de vida de identidades

- Aprovisionamiento de usuarios
- Desaprovisionamiento
- Inhabilitación rabiosa
- Gestión de perfiles de usuarios
- Gestión de credenciales
- Gestión de políticas de seguridad

Control de identidades

- Autenticación usuario/password
- Autenticación fuerte
- Single-Sign-On (Kerberización)
- Monitorización
- Auditoria

Servicios básicos de gestión de identidades

- Directorio
- Metadirectorio
- Flujos de trabajo

Situación inicial y pasos previos

Gestión de identidades

Active Directory

Notes

Siemens

DB2

Critical Path

NT

Consolidación

Sincronización

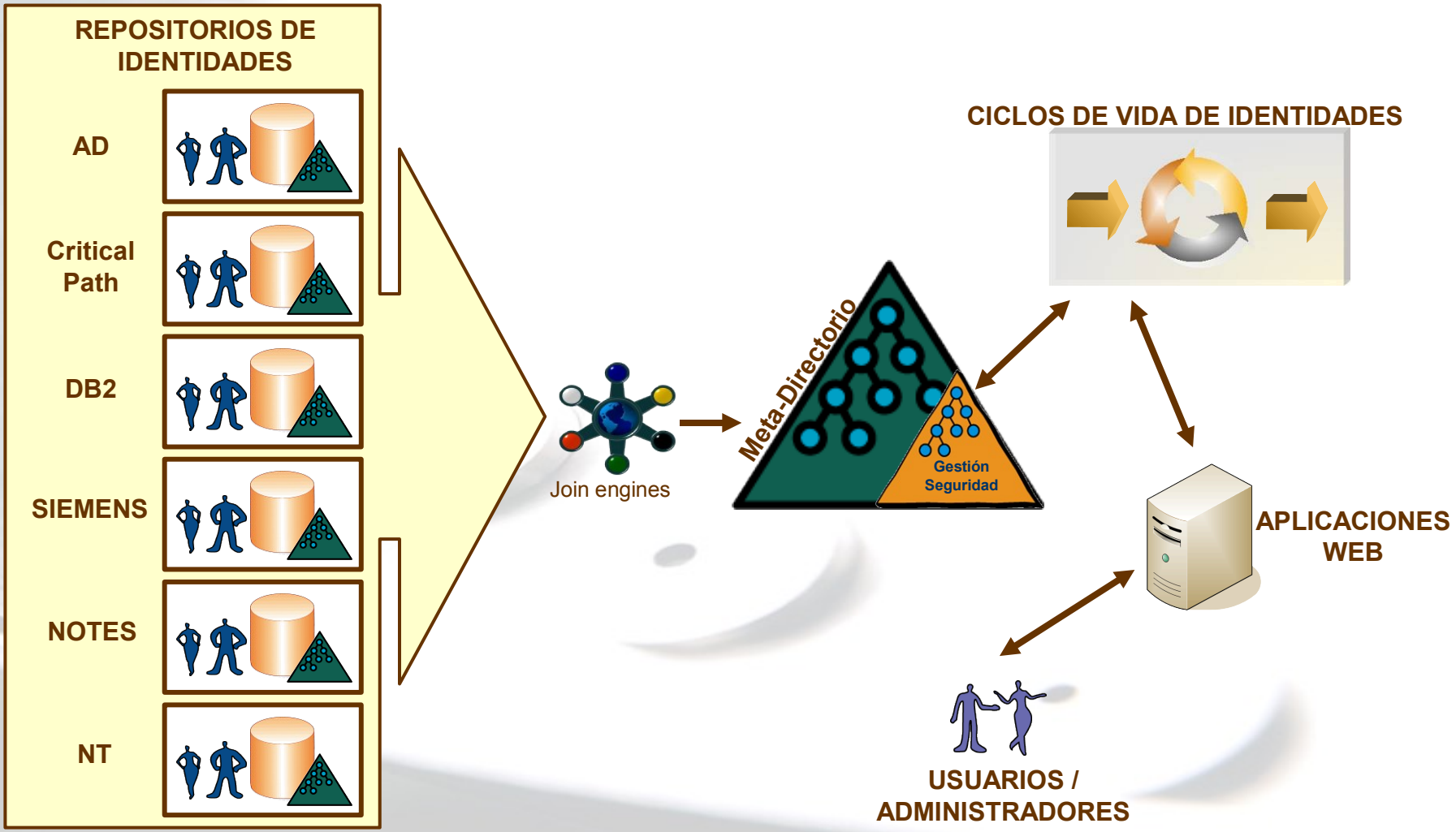
Perfilado

Funciones básicas de aprovisionamiento

Inhabilitación *rabiosa*

Situación inicial y pasos previos

Repositorios de identidades



Transformando en resultados la visión de nuestros clientes

Situación inicial y pasos previos

Requisitos de negocio

- **Cumplimento: Basilea 2, Sarbanes-Oxley (perfilado, autenticación, auditabilidad)**
- **Agilidad en la gestión de las autorizaciones: cambio de límite**
- **Limitar los costes recurrente en la administración de los sistemas de autorización**
- **Coste en desarrollo/mantenimiento seguridad de aplicaciones**
- **Apertura nuevo canal de distribución**
- **Single Sign On**

Situación inicial y pasos previos

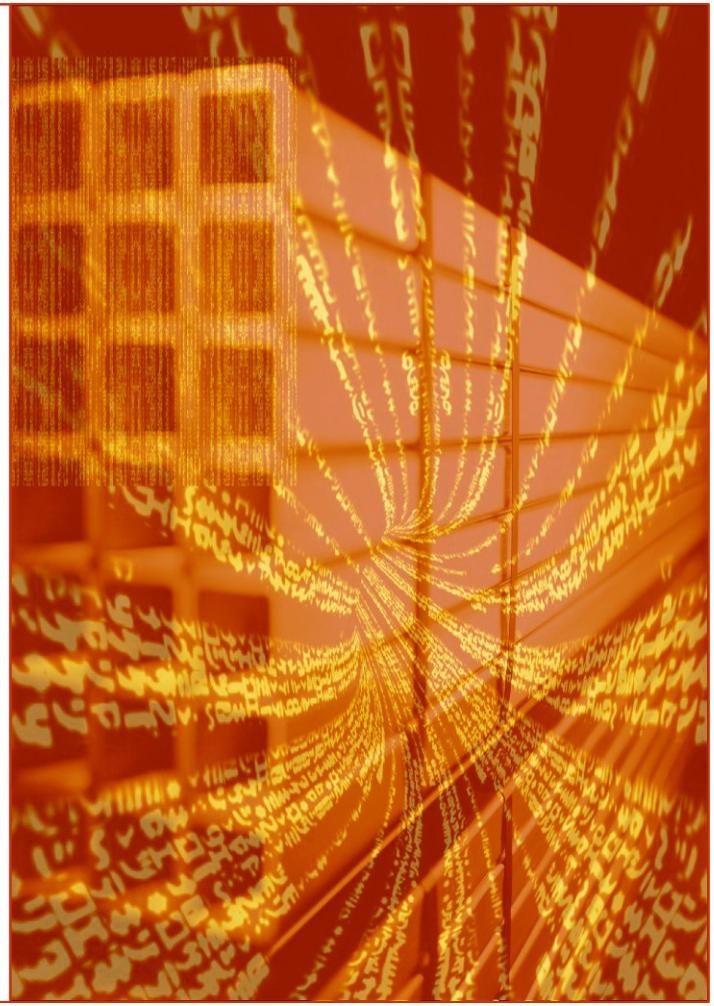
Entorno tecnológico

- Backend: Principalmente z/OS, COBOL, DB2
- Middleware: WebSphere MQ
- Frontend: AIX, WebSphere, DB2
- Plataforma multicanal J2EE (Struts)
- Active directory (Windows 2003)
- PKI Entrust, token usb Safenet
- Autenticación biométrica

Situación inicial y pasos previos

Requisitos técnicos

- Soporte de modelos de autenticación actuales
- Flexibilidad
- Modelo de habilitación universal
- Granularidad de las reglas
- Usuarios internos, administradores internos, administradores externos y clientes
- Valido para todos los Canales de Distribución
- Tecnología J2EE, JAAS, integración con WAS
- Autenticación: u/p, Cert. X509v3, token SAML
- Soporte Kerberos (SPNEGO)



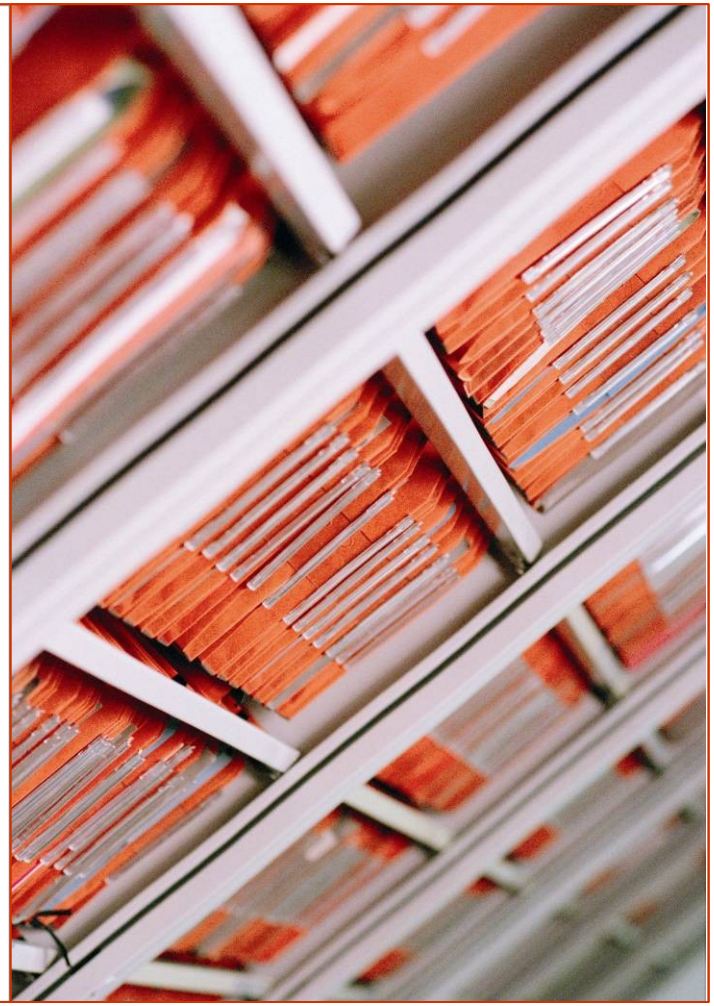
Plataforma de gestión de Accesos

Plataforma de gestión de Acceso

3 niveles de control de acceso

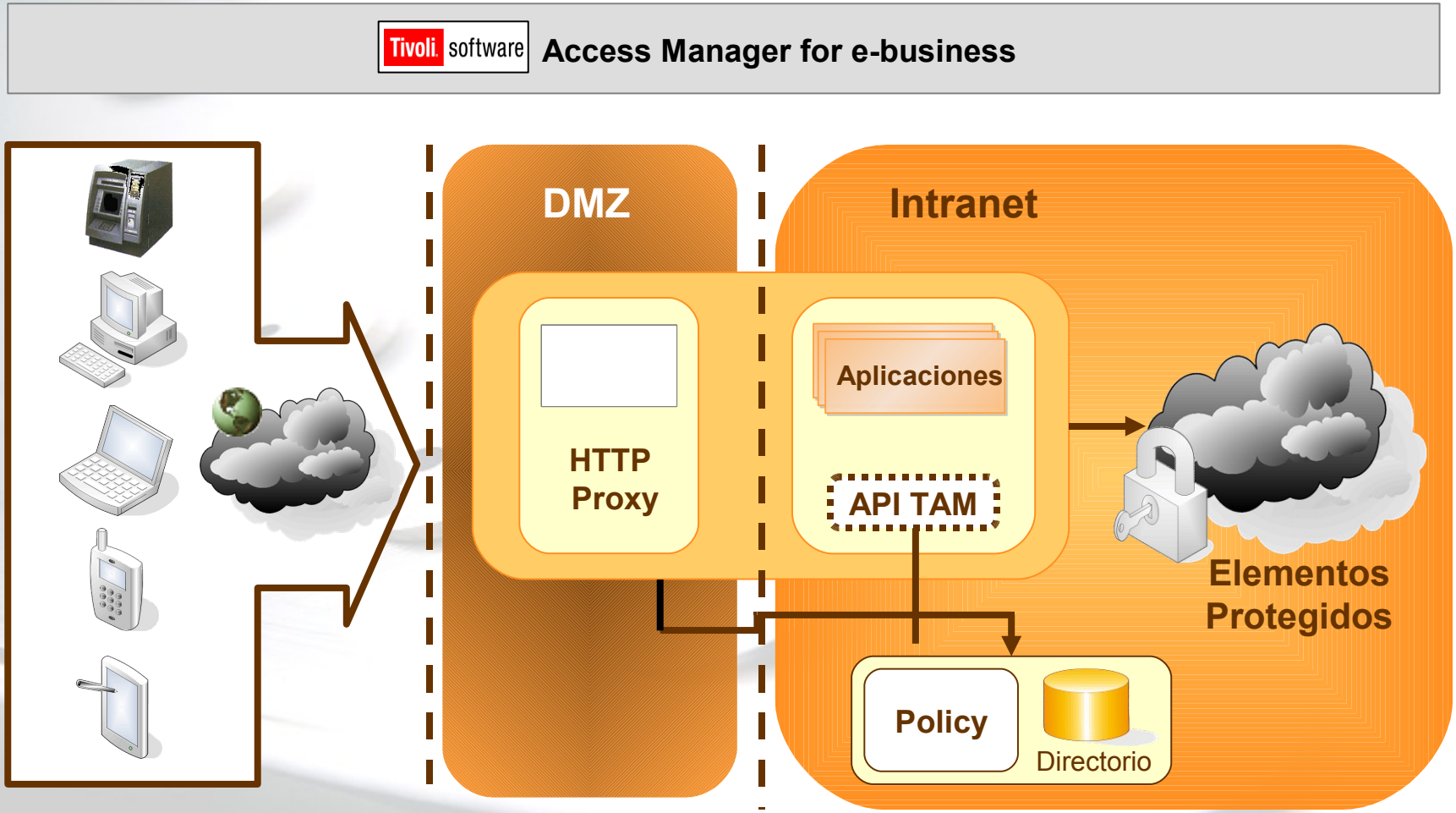
La funcionalidad requerida se puede descomponer en los 3 niveles siguientes:

- **1. Blindaje**
- **2. Adaptación UI**
- **3. Habilitaciones “grano fino”**



Plataforma de gestión de Acceso

Arquitectura General



Transformando en resultados la visión de nuestros clientes

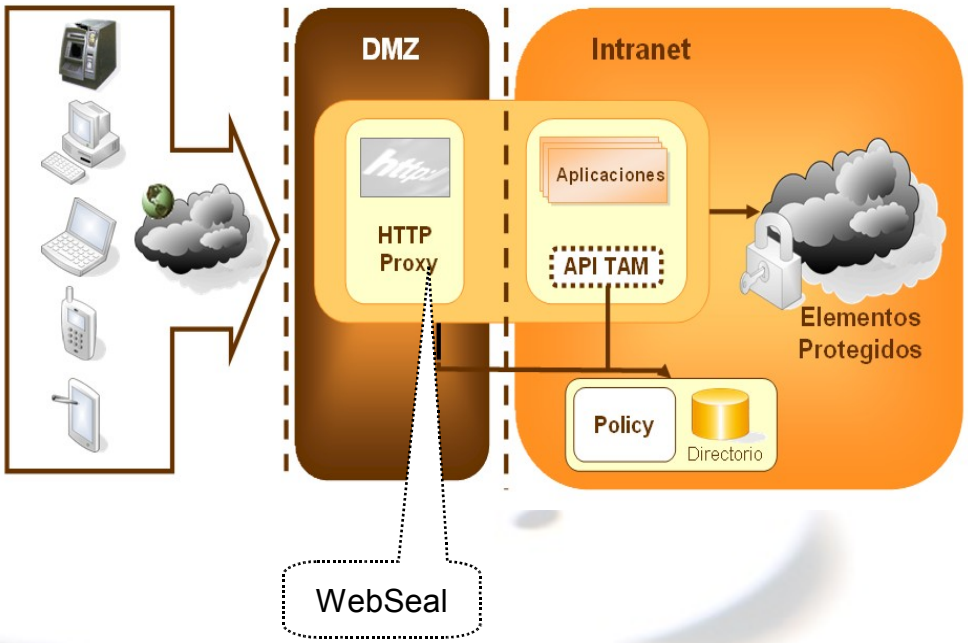
Plataforma de gestión de Acceso

Nivel 1: "Blindaje"

Tivoli software Access Manager for e-business

Funcionalidad de proxy inverso:

- **Segmentación de los recursos: Intranet, Extranet, Web Pública**
- **Realiza la autenticación de usuario, crea sesiones, alimenta el SSO**
- **Soporta delegación de la autenticación**



Transformando en resultados la visión de nuestros clientes

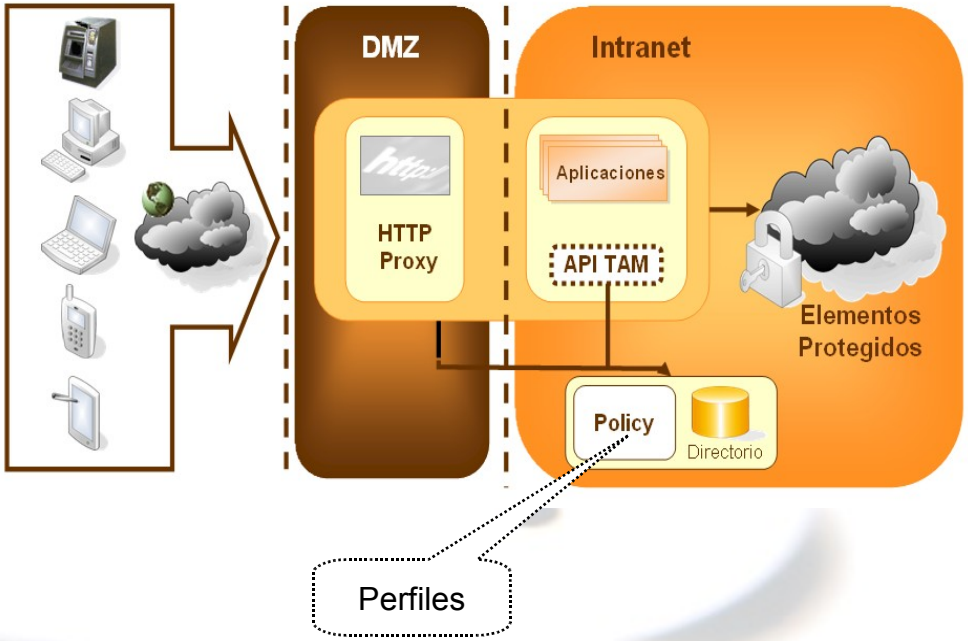
Plataforma de gestión de Acceso

Nivel 2: "adaptación UI"

Tivoli software Access Manager for e-business

Personalización del interface de usuario

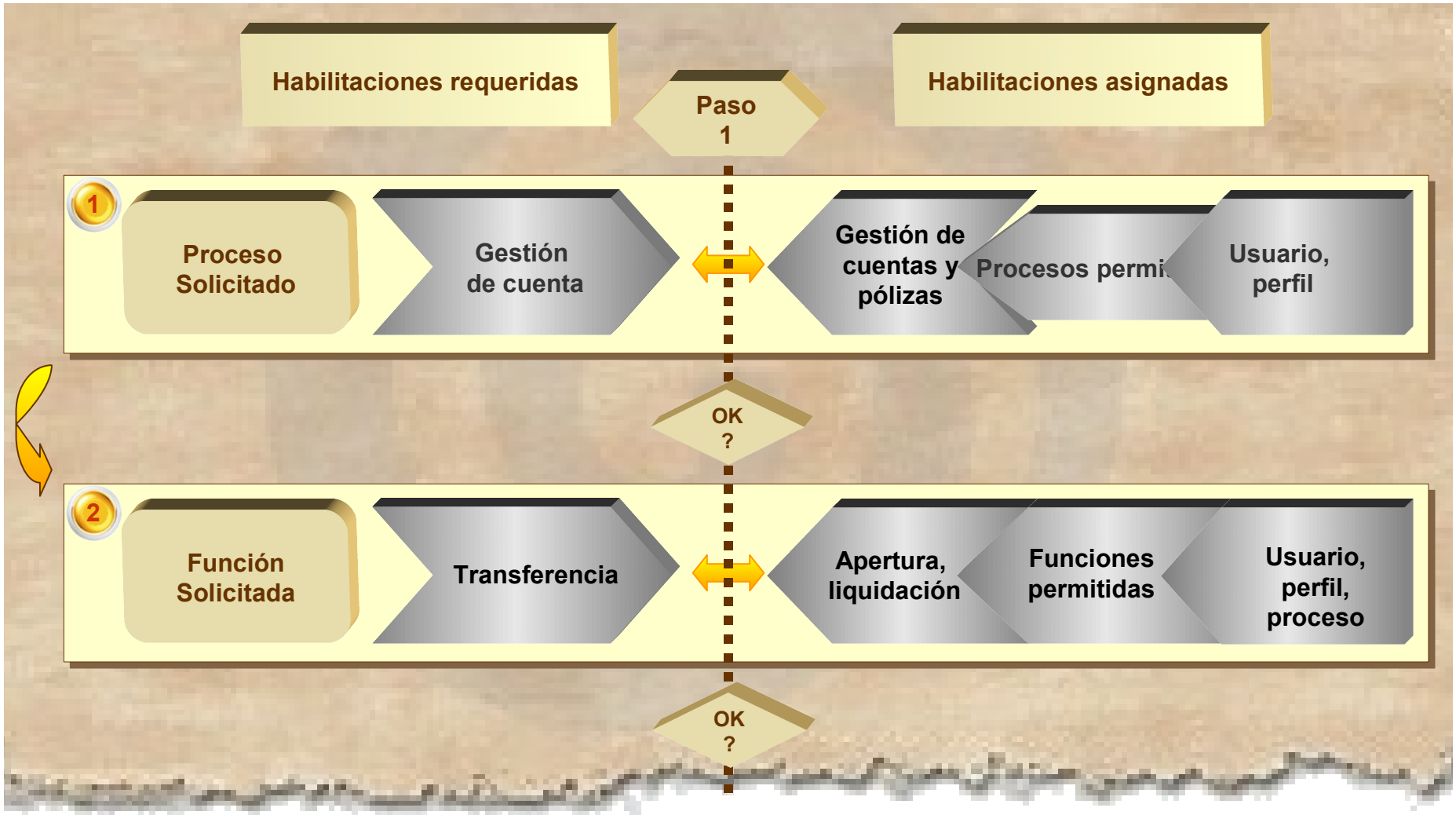
según perfil de usuario:



Transformando en resultados la visión de nuestros clientes

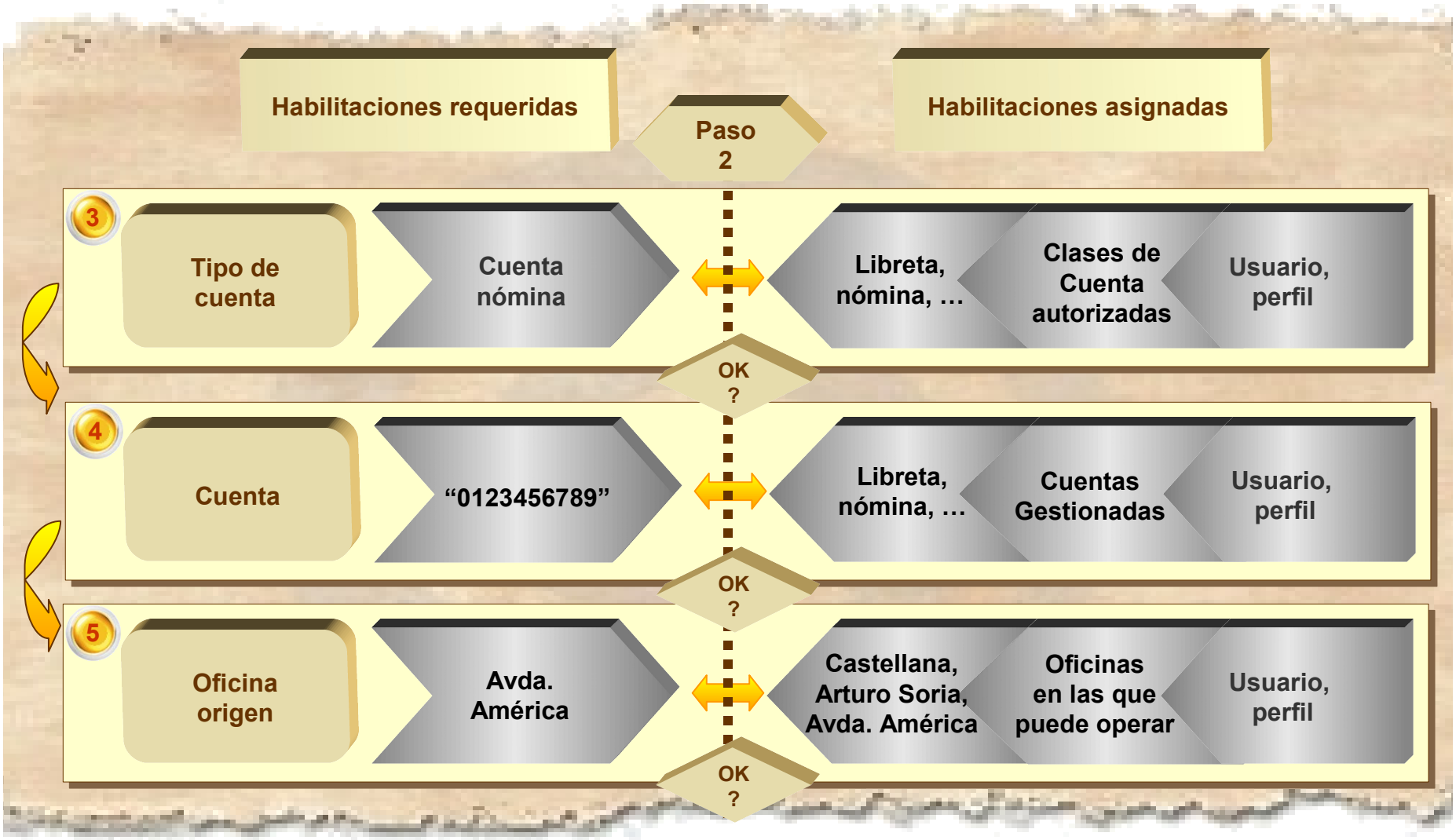
Plataforma de gestión de Acceso

Nivel 3 "grano fino": ejemplo de Proceso de Habilitación (1)



Plataforma de gestión de Acceso

Nivel 3 "grano fino": ejemplo de Proceso de Habilitación (2)



Plataforma de gestión de Acceso

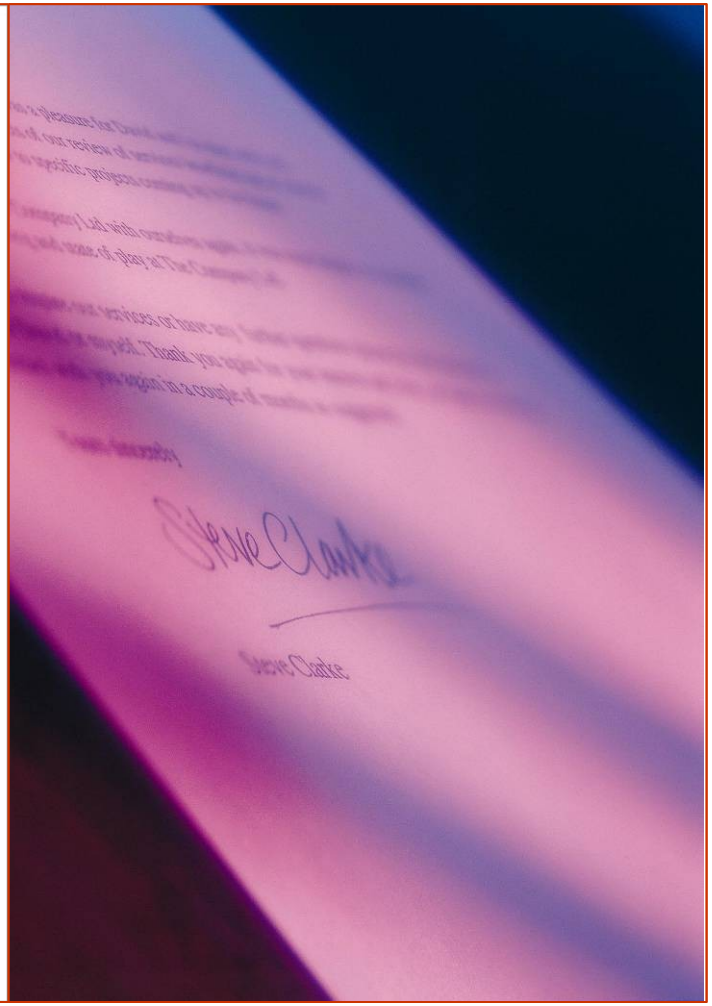
Nivel 3 "grano fino": ejemplo de Proceso de Habilitación (3)

Plataforma de gestión de Acceso

Nivel 3 "grano fino": ejemplo de Proceso de Habilitación (4)

Ejemplo de Proceso de Habilitación

- **Posibles resultados:**
  - **Se autoriza la operación**
  - **Se rechaza la operación, motivo:**
    - **La operación debe ser realizada por el gestor de esta cuenta o un apoderado**
    - **Esta operación no se puede realizar los sábados**
    - **Se han superado los limites del contato**
    - **…**
  - **La operación requiere doble firma por el director de oficina**
  - **…**



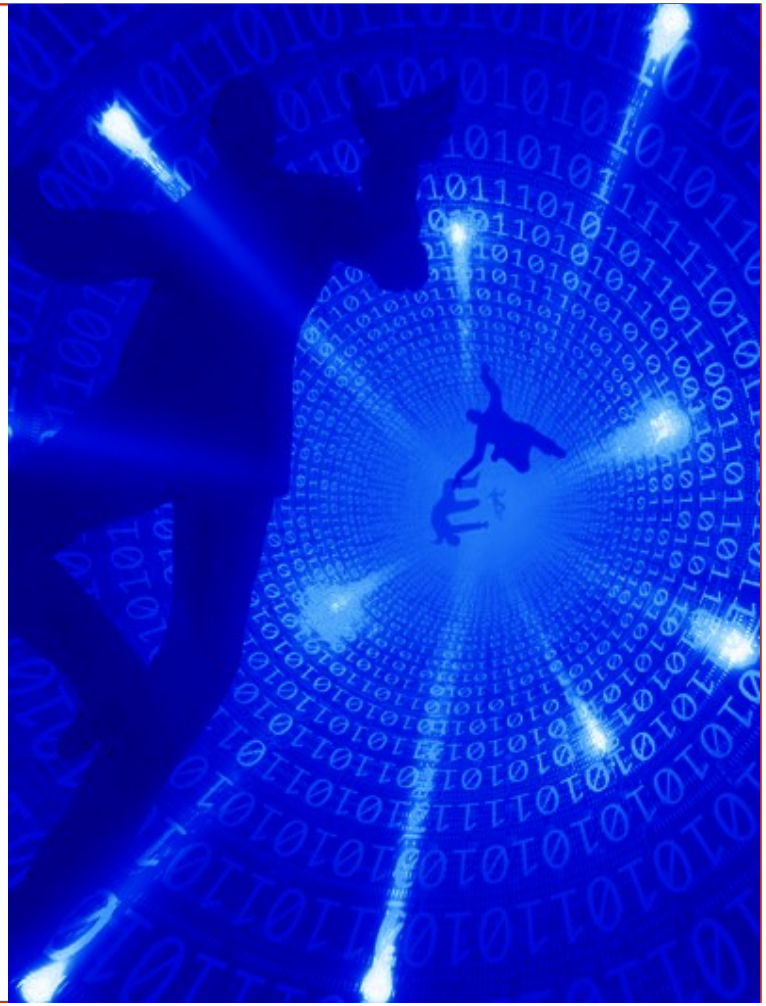
Plataforma de gestión de Acceso

Nivel 3 "grano fino"

Requisitos del Modelo de Habilitación

- ***"A final de mes, los directores de oficina están saturados, tenemos que subir los umbrales de doble firma durante este periodo"***

- **Principales características del nuevo modelo de IAM:**
  - Multi-aplicación/servicio
  - Multicanal
  - Gestión centralizada
  - No big-bang

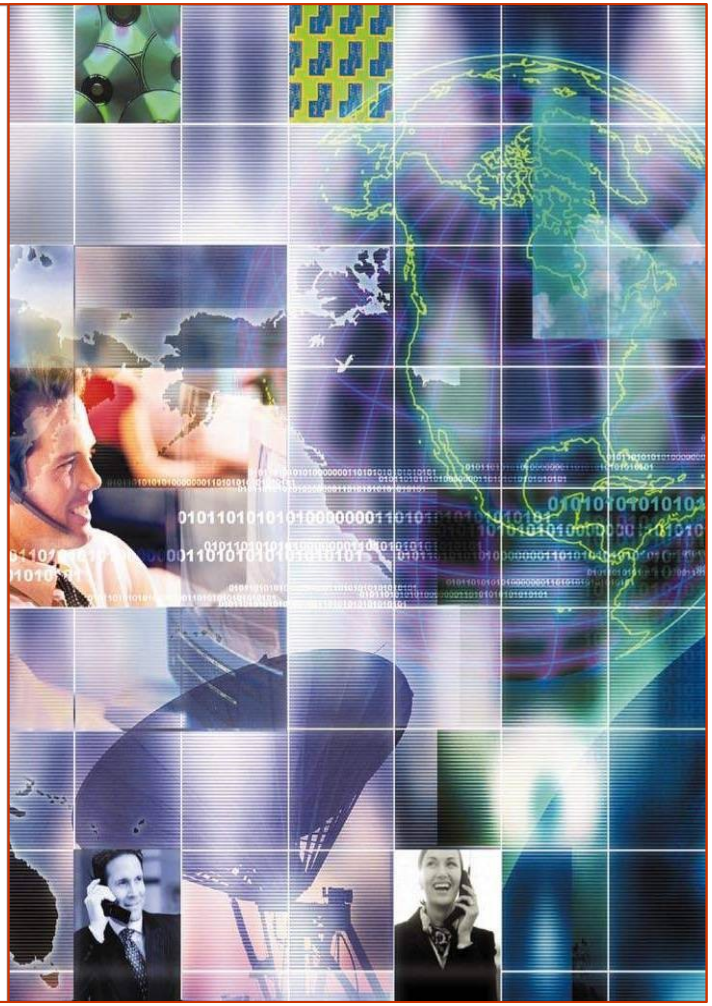


Plataforma de gestión de Acceso

Nivel 3 “grano fino”

Formalización del Modelo de Habilitación

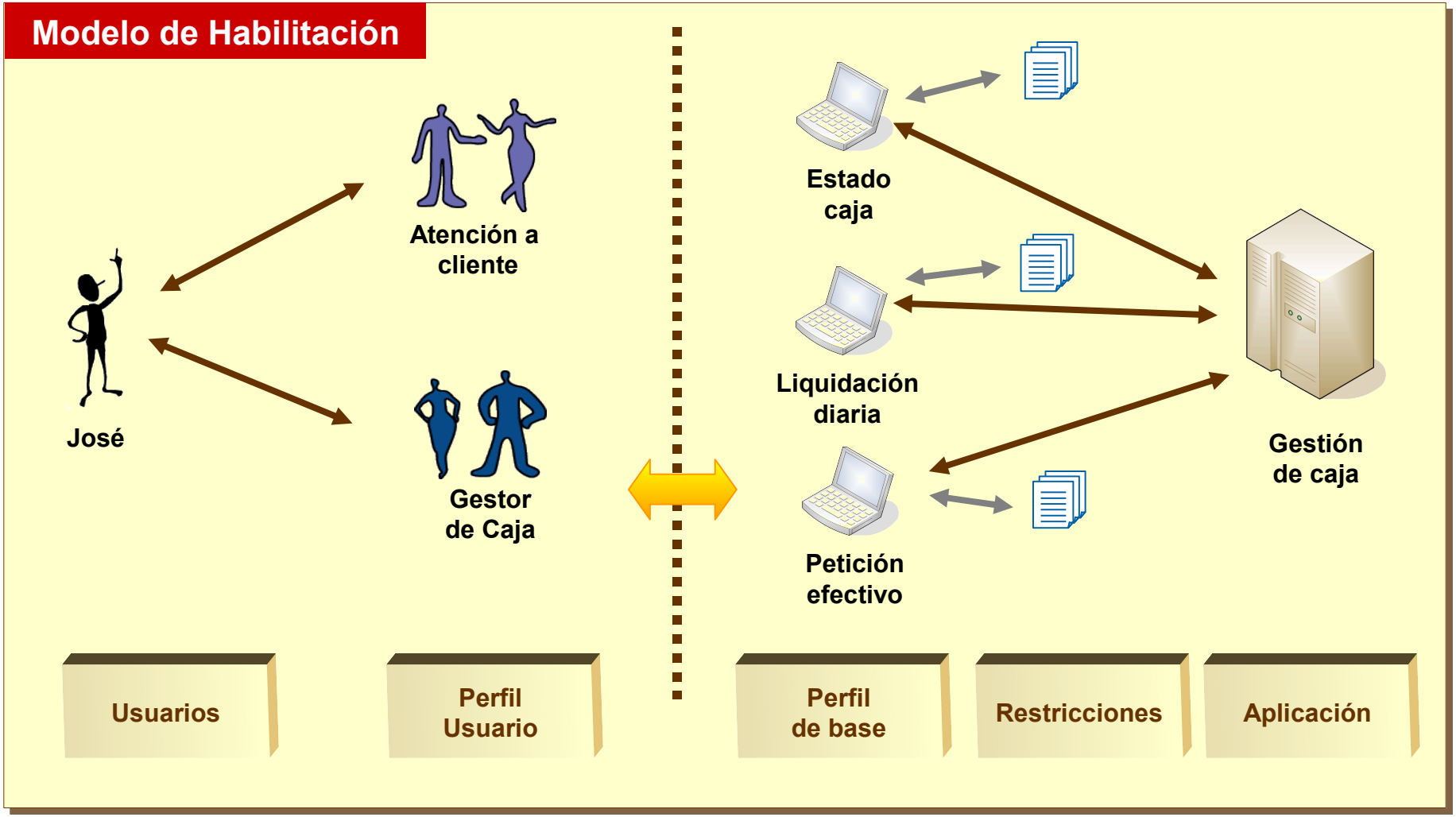
- **Usuarios**
  Pertenecen a uno o varios perfiles usuario: roles dentro de la organización
- **Aplicaciones**
  Conjunto de servicios, corresponde a los grandes procesos de negocio de la organización
- **Servicios/Operativas**
  Están asociados a un perfil básico: habilitaciones requeridas para acceder al servicio
- **Restricciones**
  Limites, umbrales, excepciones…



Plataforma de gestión de Acceso

Nivel 3 "grano fino"

Modelo de Habilitación

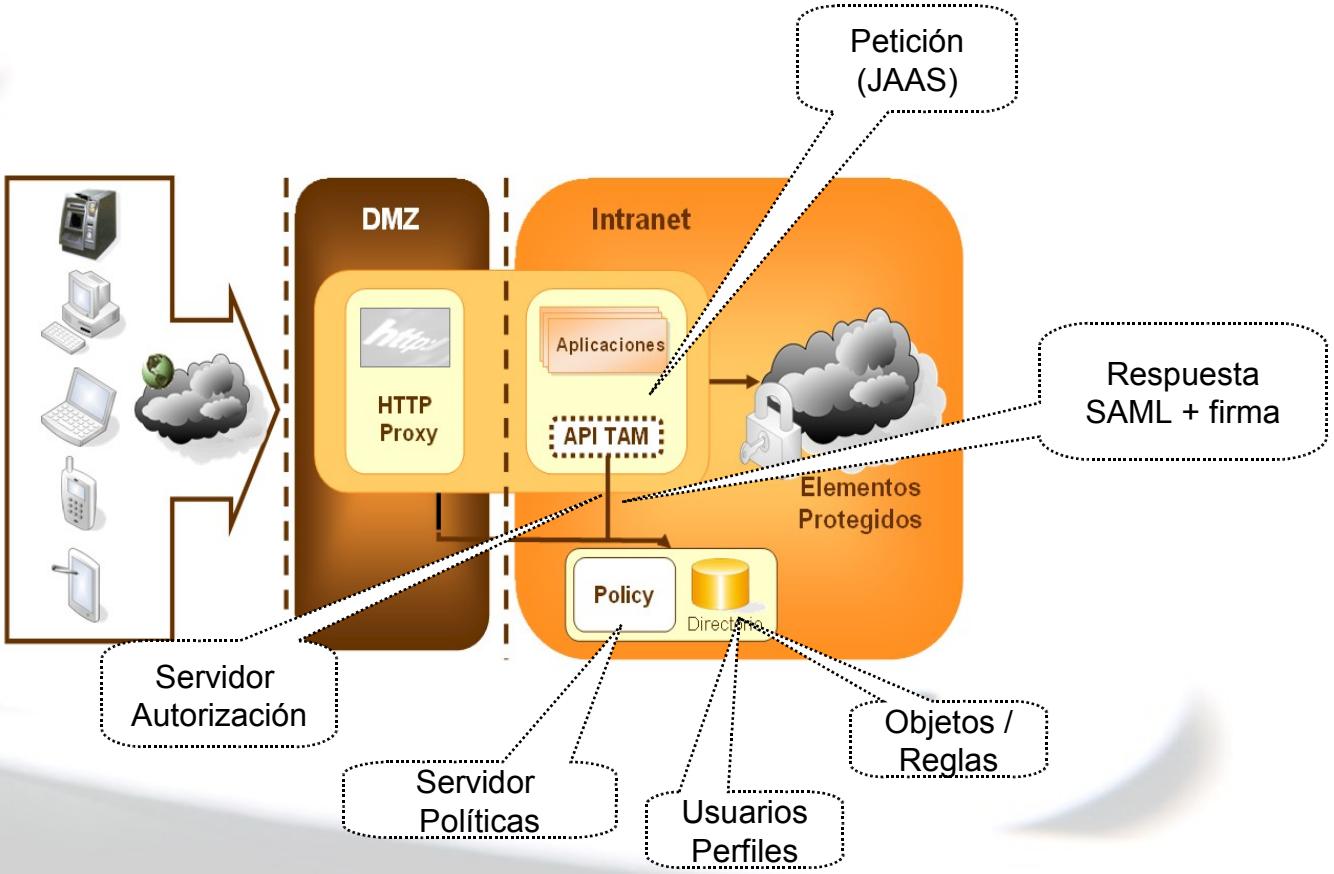


Transformando en resultados la visión de nuestros clientes

Plataforma de gestión de Acceso

Nivel 2: "adaptación UI"

Tivoli software Access Manager for e-business



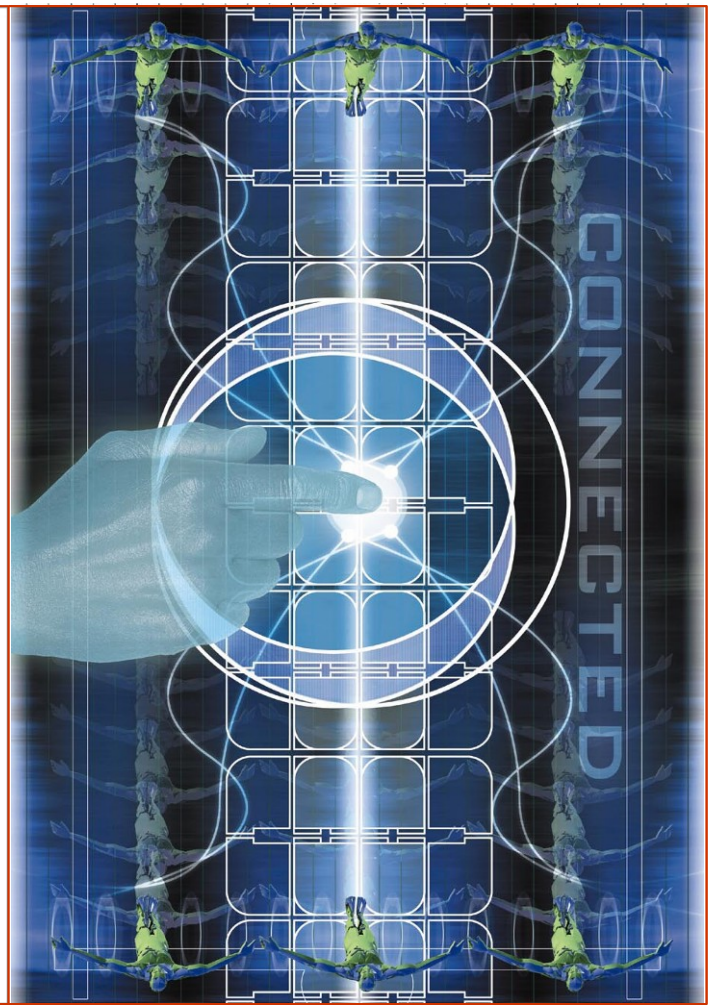
Transformando en resultados la visión de nuestros clientes

Plataforma de gestión de Acceso

Nivel 3 "grano fino"

Implementación del Modelo de Habilitación

- **Fase 1: Al nivel de cada aplicación**
- **Fase 2: Gestión centralizada a nivel de plataforma J2EE: JAAS, Token SAML, integración PKI (firma)**
- **Fase 3: Enfoque SOA: WS-***



Beneficios

Beneficios

1/2

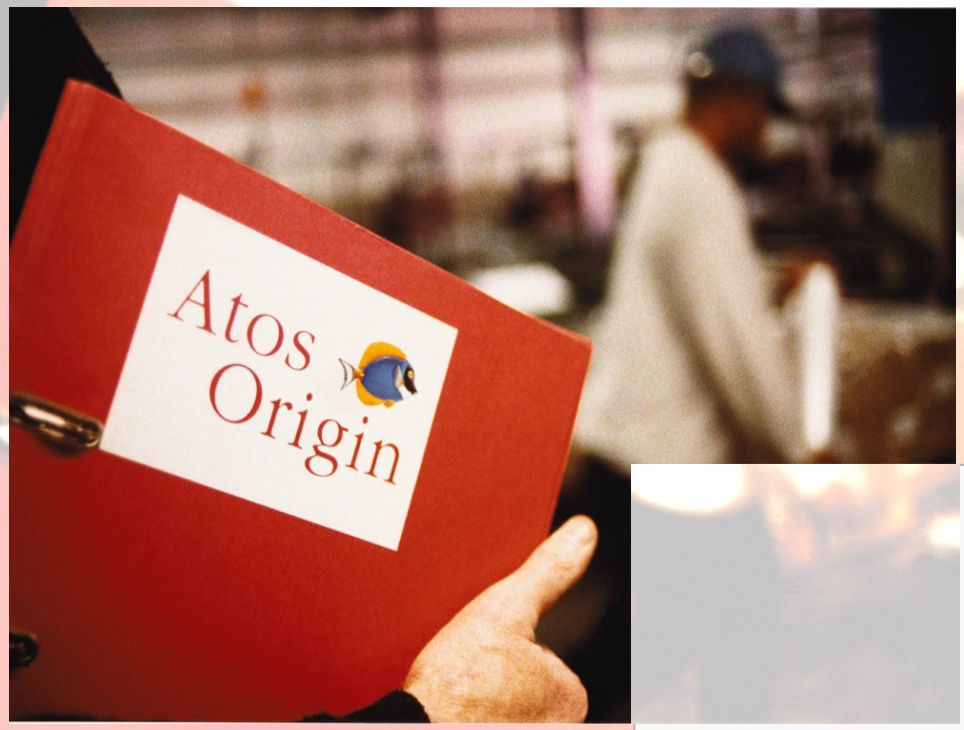
- Situación incial: dispersión de AAA, varios modelo y varias implementación
- Complejidad insostenible con el aumento de canales y procesos de negocio
- Ventajas: reducción costes de mantenimiento y aumento de la seguridad
- Se puede sacar mucho provecho de Tivoli Access Manager for e-Business… mucho mas que WebSeal…

Beneficios

2/2

- Cambio de restricciones/limites:
  - ✓ Sin impacto en las aplicaciones
  - ✓ Sin impacto en la definición de servicios y perfiles de base
  - ✓ Sin impacto en la definición de los perfiles de usuarios
- Válido para cualquier tipo de usuario
- Válida para todos los canales de distribución
- Abierto a métodos de autenticación fuerte
- Auditabilidad
- Gestión centralizada

Gracias por su atención



Contacto:

Philippe Reynaud

phillipe.reynaud@atosorigin.com