Control de Acceso en Web en Entidades de Seguros

Necesidades del negocio y Soluciones Tecnológicas

José María Jiménez De La Concepción
CISSP, CISA
Consultor de Seguridad
Víntegris S.L.

jose.jimenez@vintegris.es

Víntegris

Índice

- Nuestra Empresa
- El negocio Asegurador. Su Actividad y sus Necesidades de Servicio
- El entorno Web como herramienta del negocio. Situación y Problemas planteados
- Elementos del Control de Acceso Web
  - Funcionamiento general
  - Integración con Aplicaciones
  - Reglas de negocio
  - Autenticación Transparente de Entidades
  - Autenticación Transparente entre dominios
  - Provisión de los Usuarios
- Diversos proyectos de Control de Acceso web
- Nuestro producto OEM

- Empresa dedicada al entorno de la Seguridad de los Sistemas de Información
- Creada en 2003 con personal experto en Seguridad IT
- Nuestro personal está certificado en CISSP, CISA o CISM
- Empresa certificada por AENOR en UNE 71502:2004 (SGSI)

AENOR ER Seguridad Información SI-0006/05

- Trabajamos con múltiples tecnologías, aportando a los clientes la mejor alternativa en cada caso.

IBM Tivoli. software

betasystems

M-TECH

SPI DYNAMICS

RSA SECURITY

SecureWave Safeguarding Tomorrow

PGP

Consultoría de Seguridad

- Consultoría estratégica de Seguridad
- Diseño e Implantación de Infraestructuras de Seguridad
- Análisis y Auditoría de Seguridad de Sistemas y Aplicaciones
- Consultoría de adecuación a la certificación del SGSI

Integración de Sistemas de Seguridad

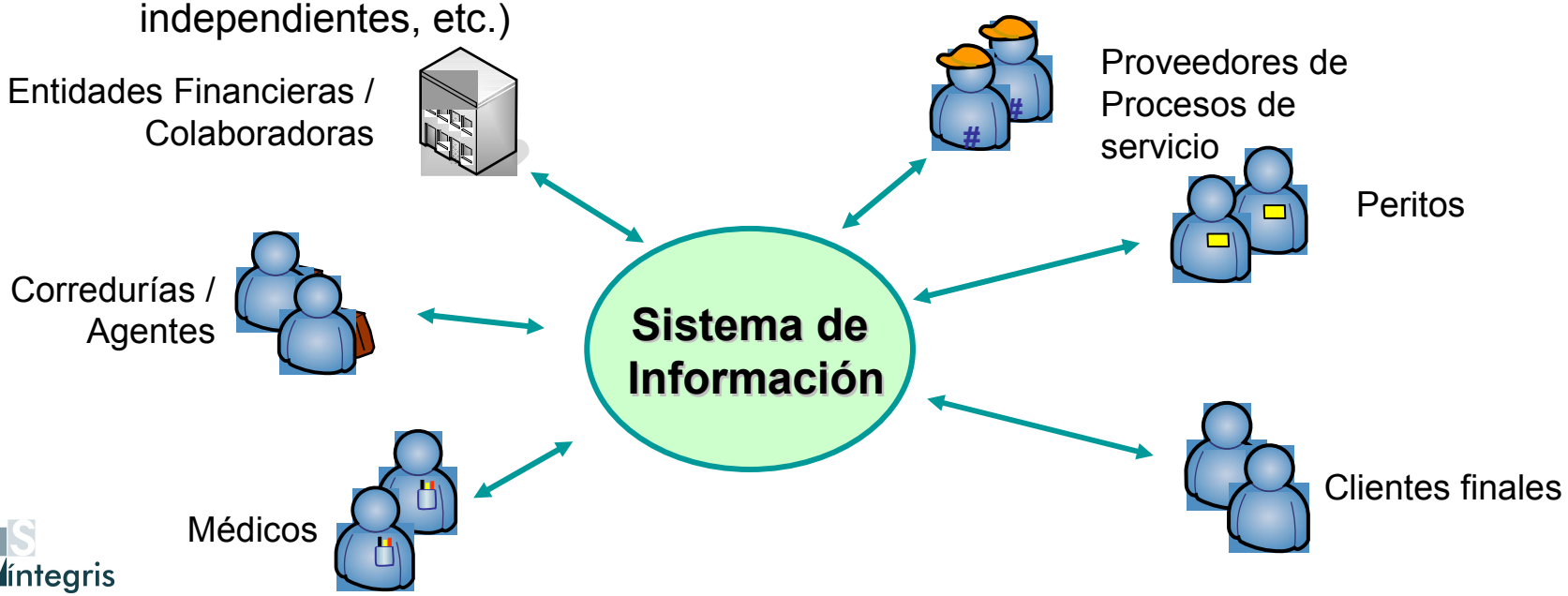
- Seguridad de Aplicaciones Web y SSO Web
- Autenticación de doble factor
- Gestión de Contraseñas
- Gestión de Aprovisionamiento de Usuarios
- Protección de Estaciones de Trabajo
- Firma electrónica

Tecnología Propia

- Correo Seguro
- Seguridad de aplicaciones Web

El negocio Asegurador. Su Actividad y sus Necesidades de Servicio

- Diferentes Actividades:
  - Comerciales/Agentes/Corredurías: Acceso al Sistema de Información.
  - Entidades Financieras: actúan como comerciales.
  - Acceso Clientes: Contratación Pólizas.
  - Peritos: Envío información peritajes.
  - Médicos: Envío/recepción documentos salud.
  - Otros proveedores o clientes: empresas que realizan una parte del proceso de peritación, certificación, ó del proceso de servicio; que necesitan acceso al Sistema de Información de la entidad. (CICOS, SIAC, peritaciones independientes, etc.)

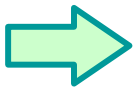


Vintegris

El negocio Asegurador. Su Actividad y sus Necesidades de Servicio

- Qué se reclama para el desarrollo del negocio asegurador:
  - Facilidad de acceso a los recursos
  - Único punto de acceso
  - Garantías de Seguridad y Auditoría
  - Disponibilidad
  - Extensión/Publicación ágil de los servicios del S.I. a proveedores de negocio.

- Problemática en la Gestión del S.I.
  - Gestión de acceso a Multitud de aplicaciones, Web y heredadas.
  - Organización de Auditoría de accesos
  - Seguridad en los accesos de cada aplicación
  - Diferentes perfiles de usuarios; diferentes necesidades de autorización.
  - Cubrir los Requerimientos legales LOPD.



El S.I. debe proveer al Negocio elementos de servicio para su normal funcionamiento y evolución futura.

Vintegris

- El entorno Web:
  - El Espacio Web se ha establecido como el entorno ideal de servicio de las necesidades del Negocio.
  - Abre el negocio al exterior, accediendo de forma fácil.
  - Publica servicios interactivos (Aplicaciones Web basadas en formularios), y servicios automatizados (WebServices).
  - El protocolo de comunicaciones es estándar.
  - Permite normalizar el acceso Intranet como Extranet.

- El entorno Web facilita el desarrollo del negocio, pero los Gestores de los Sistemas de Información se encuentran con el mismo o más grave problema de control y seguridad, que en los entornos tradicionales.

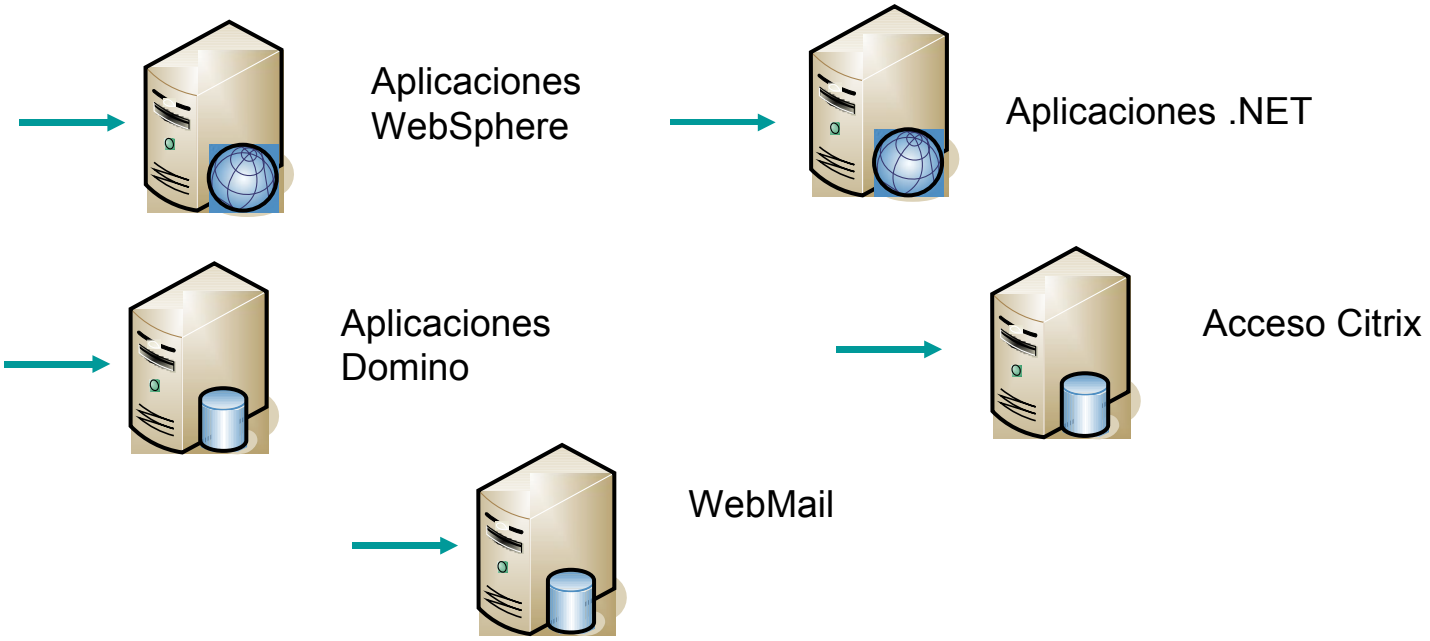
Debe plantearse un Modelo de Control para el entorno Web de la Entidad

El Modelo del Control de Acceso Web

- Los objetivos de este Modelo de Control en Web son:
  - **Homogeneizar** el espacio web común de la Entidad, para todas las aplicaciones web.
  - Establecer un **punto de entrada único** y seguro para los usuario de los servicios web
  - Establecer un sistema **centralizado para administrar** la seguridad de los recursos web heterogéneos de la compañía
  - Establecer mecanismos de **autorización** a las aplicaciones de negocio que requieran tratamientos diferenciados según el tipo de usuario.
  - **Facilitar el desarrollo** habilitando funciones de seguridad e independizando funcionalidades comunes de seguridad de las aplicaciones
  - **Habilitar mecanismos** de conectividad con terceros lo suficientemente flexible pero con las garantías de control necesarias.

El Control de Acceso Web en Aseguradoras

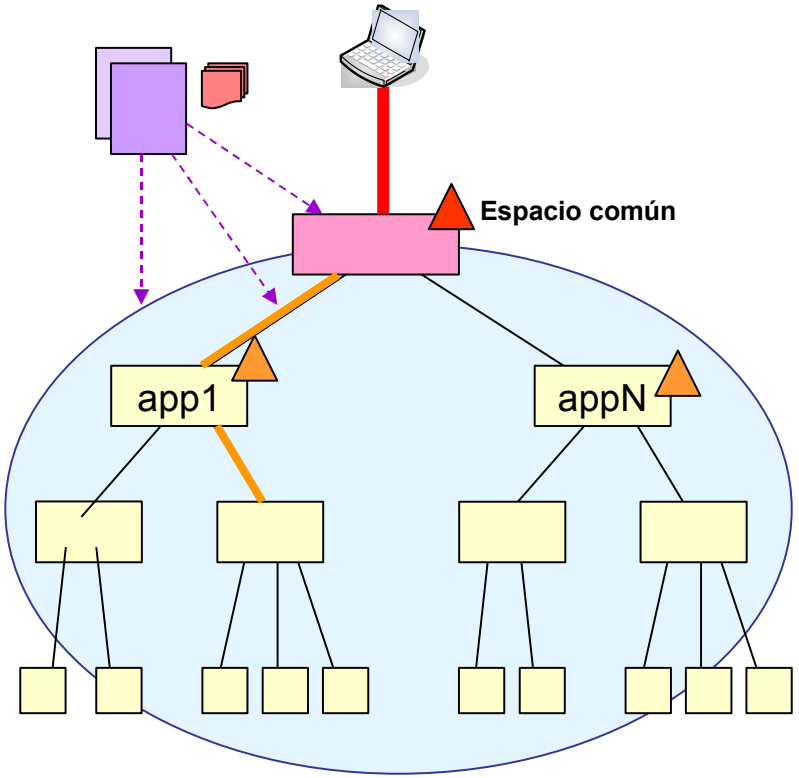
- Visión General de la situación inicial:
  - Diferentes aplicaciones web, con diferentes requerimientos de autenticación y control de acceso.
  - Cada aplicación quiere establecer su autenticación y tener su espacio web.
  - Ausencia de control centralizado para la seguridad de las aplicaciones. Cada desarrollo realiza su control de seguridad



Vintegris

Objetivos a Cubrir en los Servicios Web

Autenticación	Punto de entrada común para todas las aplicaciones
Autorización frontal	Acceso autorizado a URL según políticas centrales
Autorización de Negocio	Funciones comunes de control en las aplicaciones
Administración	Administración central del entorno
SSO web	Una única autenticación para todas las aplicaciones
Auditoría	Registro central de actuaciones
Confidencialidad	Acceso común SSL



Componentes del Sistema

- Basado en Tecnología Tivoli Access Manager (TAM)
- Adaptado a cada entidad, desarrollando elementos adicionales para cubrir todas las necesidades

Tivoli. software

WebSEAL

Proxy Frontal de Autenticación y Autorización

Repositorio/Base de datos de usuario y grupos

Sistema Central de Seguridad TAM

Azn Negocio

Módulo para el control de autorización en aplicaciones de negocio

Atn Externo

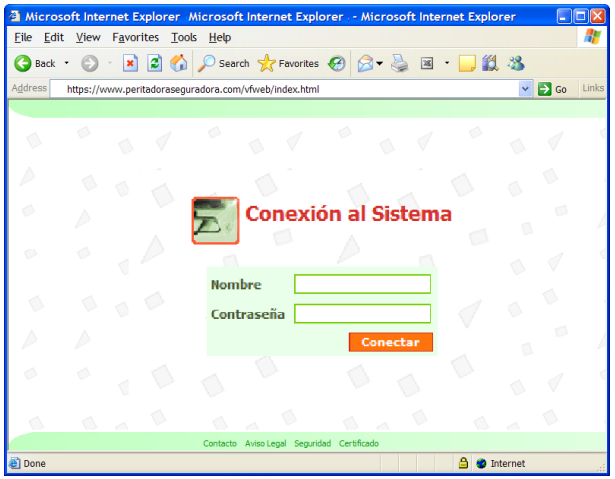
Autenticación Federada Entidades Colaboradoras

Provision

Interfaz con Administración Central

Vintegris

Flujo de Información. Autenticación y Autorización



1 Usuario se conecta a web via SSL

Internet

2 WebSEAL: Autentica al usuario si no lo estaba o comprueba su credencial

DMZ

4 WebSEAL: Autoriza al usuario a acceder a la URL

5 Aplicación: Acceso al servicio final. La aplicación podrá llamar al marco seguridad de Negocio para autorizaciones adicionales

Servidores Aplicación

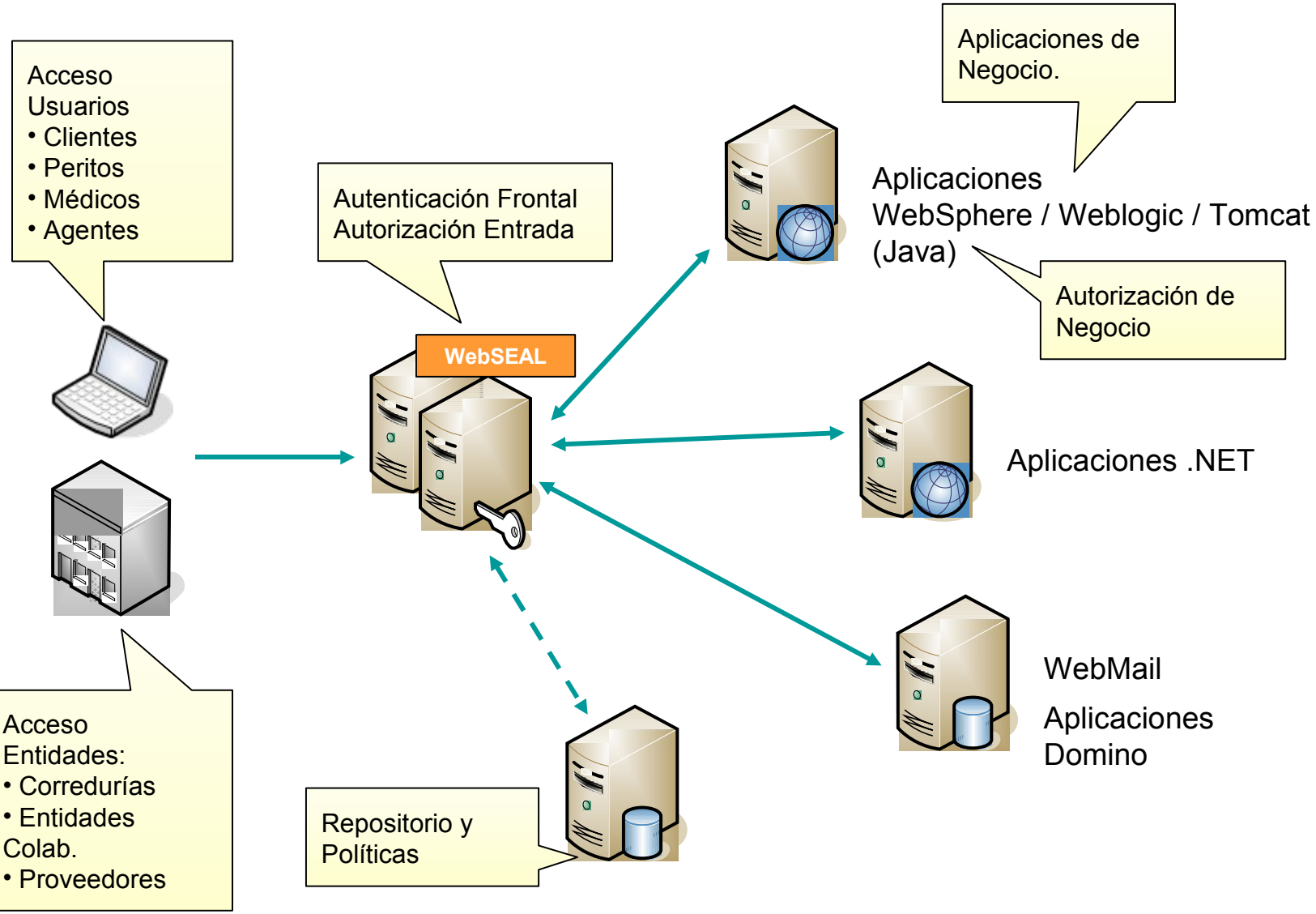
Red Interna

LDAP

3 LDAP: Es consultado por WebSEAL para autenticar al usuario y conocer sus grupos

Vintegris

Arquitectura Tecnológica

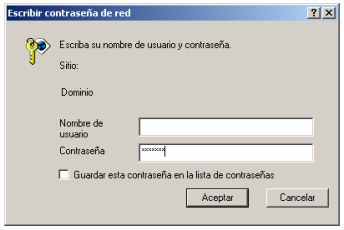


* Existen otros modelos de Integración

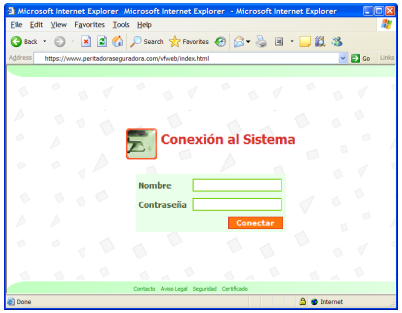
Vintegris

Tipos de Autenticación

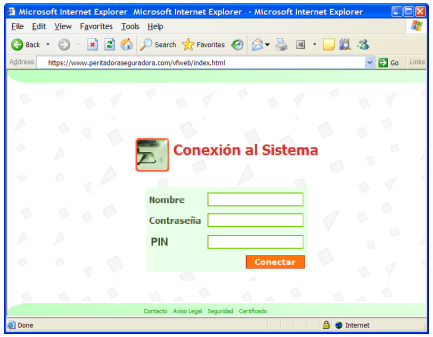
- Autenticación Básica: Información en el header HTTP
- Por formularios HTML: Información en la request o el cuerpo HTTP. Puede ser utilizando usuario/password, token, etc.
- Por certificados: Utilizando el protocolo SSL
- Otros: Desarrollados específicamente para proveer SSO.



Autenticación básica



Autenticación por formularios



Autenticación de doble factor por Token

Vintegris

Integración entre WebSEAL y Aplicaciones

- El WebSEAL puede facilitar en el header de la petición HTTP la siguiente información:
  - El userid ó el DN del usuario en LDAP
  - Los grupos a los que pertenece
  - El ID de credencial de TAM (valor interno)
  - Cualquier otro atributo que el usuario tenga en LDAP

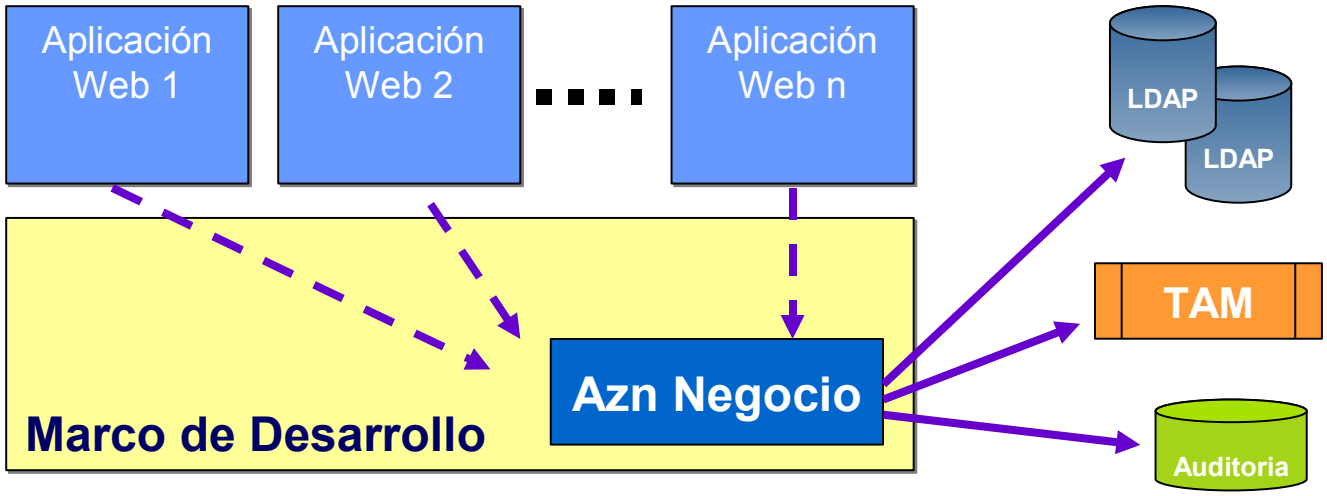
- Integración entre WebSEAL y Servicios de Aplicación:
  - Autenticación básica
  - Single Sign On en Web: WebSEAL recoge credenciales de ese usuario para el sistema final.
  - Información de Headers
  - LTPA con Domino y WebSphere

Funcionalidades Adicionales

- Proceso de Logoff
- Proceso de cambio de password. Existen políticas de seguridad en el sistema:
  - Mínimo y máximo de longitud
  - Repetición máxima de caracteres
  - Tipos de caracteres necesarios en la contraseña (9, #, A, a)
  - Histórico de contraseñas (desarrollado ex profeso)
  - Otras restricciones
- Proceso de Logon:
  - Ejemplo: con más de 5 intentos infructuosos la cuenta del usuario se bloquea por 15 minutos.

Módulo de Control en Aplicaciones de Negocio

- El objetivo del módulo de Control es proporcionar un subconjunto de **funciones y recursos** de autorización de negocio, aprovechando las capacidades de los repositorios y la tecnología.
- Este subconjunto de funcionalidades interactúa directamente con los recursos LDAP y Access Manager.
- Proporciona independencia del control de acceso con el desarrollo de la web.
- Se minimiza el tiempo de desarrollo de las aplicaciones en cuanto a mecanismos de seguridad.
- Está integrado con el marco de desarrollo de la compañía.



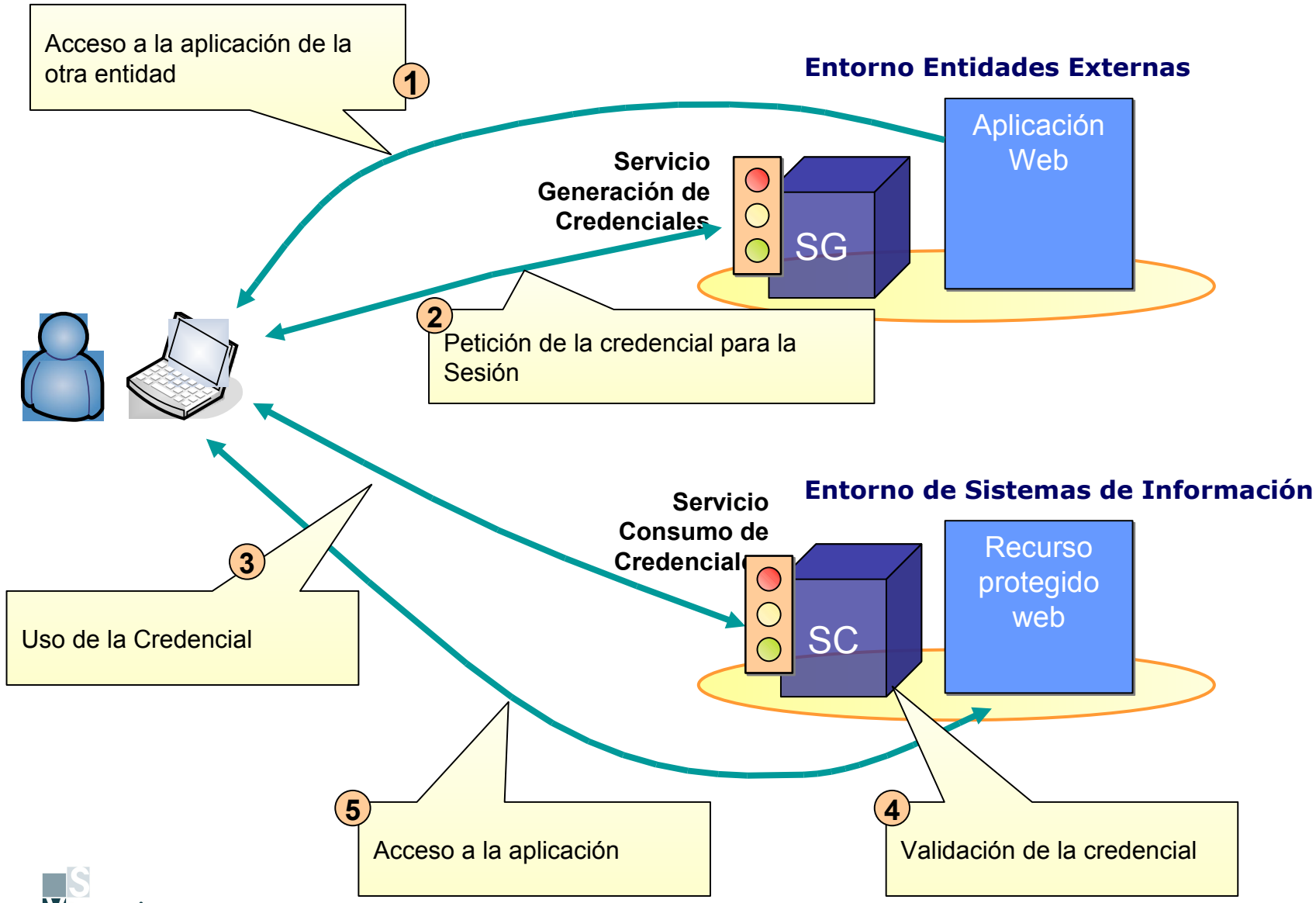
Autenticación Transparente de Entidades

- Proporcionar un servicio autenticado a usuarios/empleados de compañías colaboradoras, sin que se les requiera una autenticación explícita, pero garantizando la confidencialidad/seguridad.

- Componente que establece la relación de confianza en una entidad colaboradora, para una/varias aplicaciones web concretas. Se consigue con esto la **FEDERACIÓN DE SERVICIOS.**

- Las características de este servicio son:
  - La entidad colaboradora garantiza que aplica los mecanismos de seguridad apropiados (autenticación, autorización) para su puerta de acceso.
  - Los usuarios entran en el servicio sin necesidad de autenticación. Ésta se realiza internamente durante el proceso.
  - Se establece el acceso cifrado de la información transmitida, al margen de navegar mediante SSL
  - Se utiliza un ticket de acceso temporal en un intérvalo determinado.
  - Heterogeneidad de clientes: cgi, asp, VBScript, Tomcat, WebSphere, WebLogic, php..

Autenticación Transparente de Entidades



SSO InterDominios (SSOID)

- Caso de Grupo Asegurador: proporcionar SSO entre compañías del grupo.
- Para ello se ha utilizado la capacidad TAM para realizar la federación de servicios exclusivamente con los webseales.

- Supongamos que una página en la compañía **A** debe redirigir al usuario a otra página/aplicación de la compañía **B** sin que ésta segunda le requiera la autenticación. Los pasos a seguir son:
  - La página origen enlaza al servicio SSO intercompañías indicándole como parámetro destino la URL final. Presenta esta info al usuario
  - Cuando el usuario hace el click en el enlace, se accede al servicio SSOIC.
  - Este servicio genera un ticket y redirige al usuario automáticamente a la página destino con el ticket.
  - Con la petición de vuelta, el WebSEAL recoge el ticket y lo valida. Si es válido, no requiere al usuario la autenticación.
  - Aún cuando el usuario ha sido autenticado mediante el ticket, el WebSEAL comprueba si el usuario tiene autorización para esa aplicación.

Funcionamiento del SSO InterDominios

La aplicación **A** muestra una página con un enlace a la aplicación **B**.
"Pulse aquí para ir a la aplicación de la compañía B"

WebSEAL

Aplicación Web Dominio A

Aplicación Web Dominio B

El enlace corresponde a un recurso de WebSEAL que implementa el SSOIC.

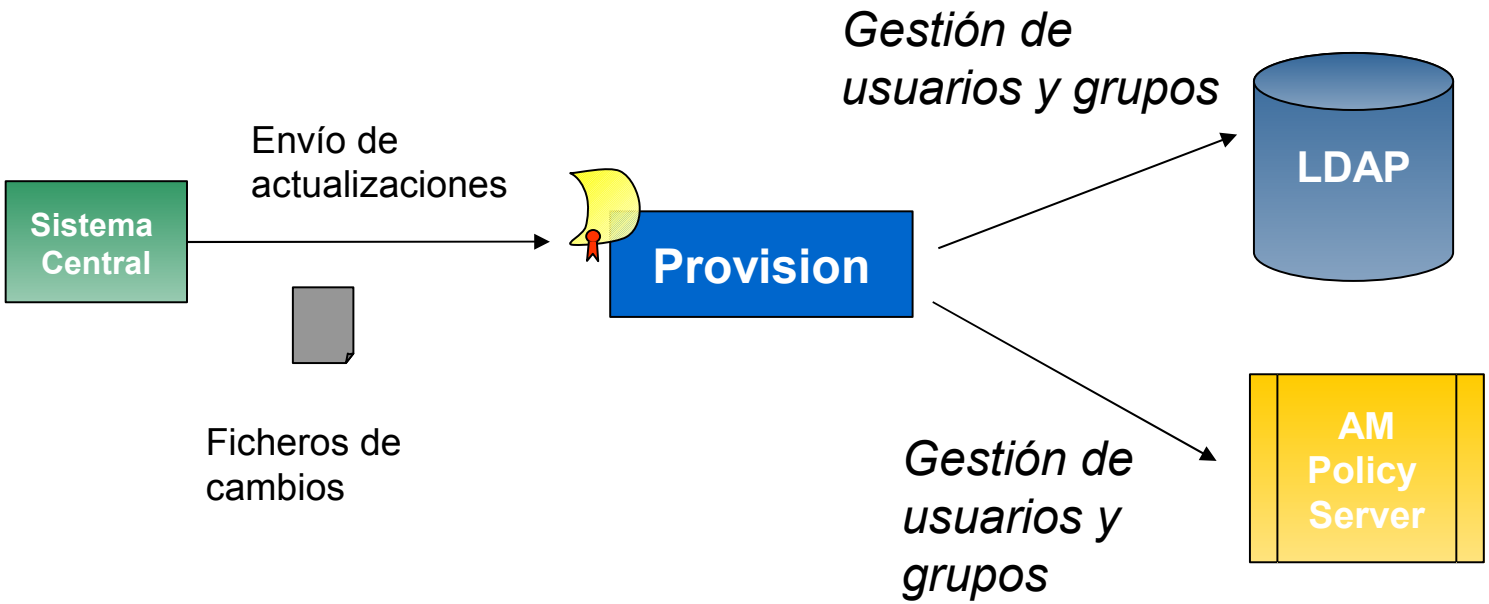
El webseal genera un ticket de acceso temporal a la aplicación destino y redirige al usuario hacia él.

El navegador del usuario pide la nueva información que le ha facilitado el WebSEAL.

El WebSEAL verifica que el ticket obtenido es correcto, está dentro del tiempo reglamentario y el usuario tiene autorización para entrar en la aplicación del **dominio B**

Aprovisionamiento de Usuarios y Grupos

- Administracion automática de usarios
- Proceso de ayuda a la herramienta del sistema central, que interactúa con LDAP y Access Manager para la actualización periódica de sus contenidos.



Otros Proyectos en el entorno del Control de Acceso en Web

- Sistema de control de acceso web para comerciales con PDA en gran empresa de alimentación.
- Sistema de control de acceso web con autenticación de doble factor RSA para banca privada, y sistema de provisión de usuarios y tokens desde sistemas medios.
- Implementación de sistemas de consistencia y administración automática para Tivoli Access Manager desde sistema de control en el Mainframe, en gran banca española.
- Sistema web de aplicación de verificaciones de estado de automóvil para empresa del sector de automoción como facilidad a empresas de seguros para aceptación de pólizas.

Nuestro Sistema de Control de Acceso Web

- En base a nuestra experiencia en el ámbito de la autenticación y autorización en las diferentes aplicaciones web y en diversos clientes, hemos desarrollado un producto **OEM**, basado en TAM como motor, incorporando elementos de control y de autenticación adicionales, tales como:

- Autenticación RADIUS, base de datos, ficheros del cliente.
- Refuerzo de políticas de contraseñas: histórico de utilizaciones, nuevas reglas, comprobación con diccionarios, etc.
- Sincronización de contraseñas: cambio directo en otros LDAP de la corporación e integración con productos de gestión de contraseñas.
- Módulos de reglas de negocio (personalización)
- Integración con Módulos de provisionamiento (personalización)

Preguntas