Universidad Latinoamericana de Ciencia y Tecnología

ULACIT

Licenciatura en Informática con Énfasis en Desarrollo de Software

Artículo:

Análisis Teórico-Técnico de Single Sign-On

Autor:

Harold González Gamboa / 1-1132-0075

Profesor:

Guillermo Oviedo B.

Tercer Cuatrimestre, Año 2005

ANÁLISIS TEÓRICO-TÉCNICO DE SINGLE SIGN-ON

Harold González Gamboa[1]

Resumen

El presente artículo describe el análisis teórico-técnico del single sign-on, en el cual inicialmente se detalla la problemática que enfrentan algunas empresas con la administración de la autenticación del usuario, la cual no es llevada a cabo de forma adecuada provocando efectos negativos en las empresas y debilitando la seguridad de los recursos. En base a esto se describe el concepto de Single Sign-On como una solución al problema, ventajas, desventajas, y además se presentan varias arquitecturas que pueden ser implementadas en las organizaciones con sus respectivos componentes. Estas arquitecturas descritas son: Password vault, Administración centralizada con almacenamiento local de credenciales, Administración y almacenamiento de credenciales centralizados, Arquitectura SSO totalmente distribuida y Administración y almacenamiento de credenciales centralizados garantizando alta disponibilidad y redundancia. Finalmente, se brindan algunos nombres de productos en el mercado disponibles para empresas que deseen implementar una solución SSO.

---

[1] Bachiller en Ingeniería de Sistemas. Candidato a Licenciatura en Informática con Énfasis en Desarrollo de Software, ULACIT. Correo electrónico: hagonzalez@ice.go.cr

Abstract

The present article describes the technical-theoretical analysis of the Single Sign-On in which the problematic that some enterprises face with the authentication of the user are initially detailed, which is not conducted in a correct management, causing negative affects in the enterprises and weakening the security of the resources. Then the concept of the Single Sign-On as a solution to the problem, advantages and disadvantages, also several architectures are presented which can be implemented in the organizations with the respective components. These architectures described are: Password vault, Centralized administration with the local storage of credentials, Administration with storage of centralized credentials, SSO Architecture totally distributed and Administration and storage of centralized credentials under guaranteeing high availability and redundancy. Finally the names of some products available in the market for enterprises that desire to implement an SSO solution.

Palabras Claves.

Single Sign-On, Seguridad, Autenticación, Autorización, Arquitecturas.

Índice

Introducción.

Hoy en día en las organizaciones, uno de los objetivos más importantes a tomar en consideración, es el poder llevar a cabo un control adecuado de la seguridad, esto se debe al gran número de amenazas que ponen en peligro los recursos de la institución, por lo que se pretende disminuir los riesgos o el impacto que pueden tener estas sobre la misma. La mayoría de las empresas velan por la protección de todos sus activos, por lo que trabajan por mejorar la seguridad realizando estudios con el fin de conocer las debilidades de la empresa e implementando los procesos para mejorar los controles de seguridad constantemente.

Un activo al cual se le brinda gran importancia, es la información de la organización, ya que se debe velar por evitar la mala distribución de esta debido a que podría afectar el negocio si cayera en manos inadecuadas. Para brindar a la información la seguridad apropiada, se deben definir los procesos óptimos a seguir para alcanzar la administración integral de la seguridad, que se refiere a todo un modelo de seguridad que inicia desde la definición de las políticas generales en base a los requerimientos de negocio definidas por la gerencia, con lo cual posteriormente se pueda realizar el análisis de los riesgos, la realización de un plan entre lo que se puede tomar en cuenta la definición de las políticas específicas de seguridad, el desarrollar este plan, el operarlo y medirlo finalmente para conocer que tan beneficioso resultó, todo esto anterior siempre buscando cumplir los requerimientos de negocio.

Con un modelo similar a este, las organizaciones pueden brindar servicios de seguridad sobre la información, los cuales deberán ser debidamente administrados para facilitar una seguridad adecuada. Dos servicios a los cuales se les debe brindar suma importancia con respecto a su administración, debido a la protección que brindan a la información, son la autenticación y autorización, por lo que surge el concepto Single Sign-On como una de las tecnologías para dar mayor facilidad en la dirección total de dichos servicios, brindando control sobre los accesos que poseen los usuarios de la empresa que requieren acceder a los sistemas, aplicaciones o bases de datos con los que cuenta la institución para brindar la información de interés para las labores diarias de cada empleado.

Con el presente artículo, las empresas podrán conocer en que consiste el Single Sign-On, así como también los diferentes aspectos importantes a tomar en cuenta para implementar esta solución en su empresa. Además se darán a conocer los problemas que tienen las organizaciones en la actualidad y que podrían ser controlados mediante esta solución para que las instituciones hagan conciencia de lo necesario y útil que puede ser el contar con el SSO.

Problemática.

Actualmente las empresas tienen grandes dificultades con respecto a la dirección de la identidad del usuario, ya que una vez que se da un nuevo ingreso de un empleado a la institución, se torna complicado el brindarle a este los permisos de acceso a todos los recursos que empleará en su trabajo debido al gran número de aplicaciones, sistemas y demás recursos de la empresa. Esto anterior no solo se presenta con usuarios internos, también las empresas requieren proporcionar permisos a usuarios externos, ya sean estos clientes, vendedores o socios comerciales, los cuales también requieren utilizar ciertos servicios de la institución por lo que se les debe brindar los accesos necesarios.

Este primer obstáculo que enfrentan las empresas con el registro de nuevos usuarios, le puede restar beneficios, ya que este proceso puede tardar una o hasta más semanas, con lo cual los usuarios pierden productividad mientras esperan por el acceso a los recursos. En algunas ocasiones este tiempo se reduce pero con un gran riesgo de la seguridad de los recursos, ya que el personal administrador brinda demasiados accesos al no definirlos de acuerdo al perfil del usuario con el fin de agilizar el aprovisionamiento y esto puede ser aprovechado por parte de los usuarios para fines que puedan afectar a la institución.

Conforme pasa el tiempo, esta situación se vuelve más compleja debido a que las organizaciones incrementan el número de aplicaciones en su infraestructura de tecnología de información, y al igual que las demás deben estar protegidas permitiendo acceso

solamente a las personas indicadas. Este problema presentado con el aprovisionamiento se debe a que las aplicaciones cuentan con un componente de seguridad para cada una de ellas, por lo que se requiere administrar las credenciales de los usuarios, los roles que tendrán estos, permisos de acceso y otros datos personales del usuario.

Además de que la empresa tiene que afrontar el conflicto en el aprovisionamiento descrito anteriormente, también se presentan complicaciones para los usuarios ya que estos deberán aprenderse sus contraseñas y darles el mantenimiento debido para brindar la seguridad apropiada a los recursos utilizados, lo cual en algunos casos complica al usuario ya que tiene que memorizar gran cantidad de identificaciones y realizar el mantenimiento de las mismas cada cierto tiempo, lo que se hace muy lento debido a que tienen que actualizar todos sus credenciales e información personal para cada una de las aplicaciones a las cuales tienen acceso, por lo que en algunos casos esto se realiza inadecuadamente.

Otro inconveniente que tienen las instituciones, es el lograr una correcta administración de las identificaciones ya existentes en el sistema, ya que además de que los permisos de acceso aumentan día con día, también muchos accesos deben ser eliminados una vez que los usuarios ya no requieren de estos, o luego de que ya no laboren para la institución. Esto último se ha convertido en una tarea difícil al contar con tantos registros en toda la infraestructura de tecnología ya que dificulta la eliminación total, por lo tanto quedan en el sistema identificaciones de usuarios que ya no trabajan para la institución lo cual hace muy vulnerable el control de acceso a la información.

Definición de Single Sign-On (SSO).

El Single Sign-On es un proceso por medio del cual se puede llevar a cabo toda la administración de control de acceso de las diferentes plataformas de la organización, y funciones de autenticación y autorización en una sola y centralizada función administrativa.

Este permite realizar la función de todos los componentes de seguridad de los recursos de la empresa desde un solo servicio SSO. Mediante este servicio, el usuario podrá autenticarse y registrarse en el sistema solamente una vez con lo cual podrá acceder a todos los recursos sin tener que volver a identificarse debido a que todos los dispositivos de seguridad están centralizados en el SSO y además podrán ser debidamente administradas las credenciales de cada uno de los usuarios para todas las aplicaciones o servicios disponibles.

El Single Sign-On no se debe confundir con la sincronización de contraseñas ya que en este no se requiere definir de igual forma todas las credenciales que utilizan los usuarios para cada aplicación o servicio, al contrario permite poseer diferentes contraseñas para cada uno de los recursos pero controlando el acceso a estos mediante una sola identificación de usuario.

Implementación del SSO.

Para implementar un servicio de SSO en una determinada empresa, esta deberá tomar en consideración diferentes aspectos tales como los recursos computacionales y económicos disponibles, ya que hay diferentes tipos de arquitectura que pueden brindar una solución de Single Sign-On, pero cada una de estas requiere que la empresa posea diferentes recursos para implementarla. Debido a esto, es recomendable que las organizaciones adquieran conocimiento acerca de las diferentes arquitecturas SSO, esto con el fin de que mediante las características, ventajas y desventajas de cada una de estas y los recursos que requieren, las organizaciones tengan la facilidad para la selección de la arquitectura más recomendable para su empresa. Por esta razón se brindará la información referente a los diferentes diseños de arquitecturas SSO.

Todas las arquitecturas que se pueden implementar en las organizaciones, constan de tres componentes importantes, los cuales serán descritos en seguida para facilitar la descripción de cada una de las arquitecturas:

- La interfase: ésta es conocida como el Agente SSO, la cual se localiza en el cliente y permite que SSO interactúe con las aplicaciones, además se encarga de almacenar en una base de datos o directorio protegido, las credenciales que le permiten al usuario acceder a cada una de las aplicaciones o servicios de la empresa.

- La administración: este elemento es por medio del cual se realiza la configuración, mantenimiento y monitoreo del proceso SSO. La ubicación desde donde se realice esta, depende de la arquitectura implementada, ya que puede llevarse a cabo desde el cliente o desde un servidor en la red.
- Las credenciales de usuario: Esta es la información confidencial del usuario para poder acceder a las aplicaciones, la cual es el nombre de usuario y la contraseña, pero además de estos datos, se almacena otra información personal del usuario. Toda esta información solo debe ser accedida por el Agente SSO y se encuentra ubicada dependiendo de la arquitectura empleada, esta puede ser en el cliente mismo, o en una base de datos central.

Arquitecturas.

1. Password vault.

Esta arquitectura requiere de una configuración muy básica, en esta los tres componentes mencionados anteriormente se encuentran en el cliente por lo que se deben acceder a las aplicaciones desde allí. Primeramente se registran las credenciales que el usuario requerirá para posteriormente ser brindadas a las aplicaciones que lo soliciten cuando el usuario desee accederlas. “Ver Figura 1”

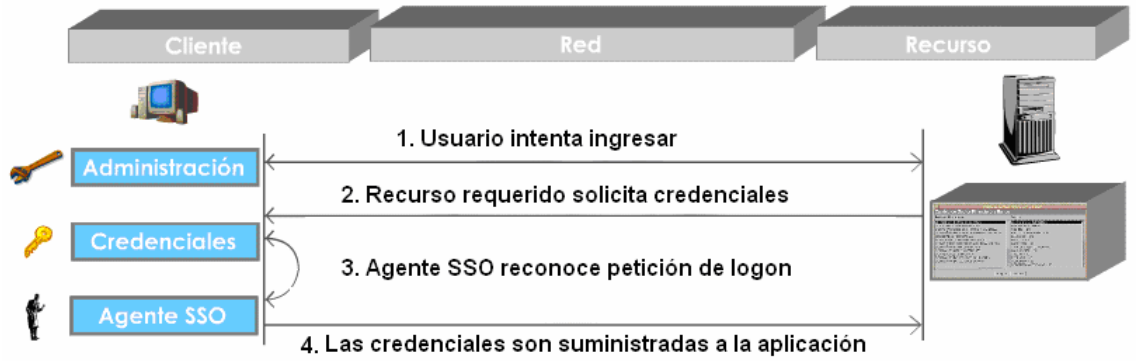

Figura 1

Fuente: http://www.criptored.upm.es/guiateoria/gt_m142j.htm

Ventajas.

- La implementación de este diseño no es complicada para la empresa, ya que no consta de tantos recursos por configurar.
- No requiere de muchos recursos computacionales, ya que solamente se deben poseer un servidor central donde residen las aplicaciones y los clientes necesarios.

Desventajas.

- La administración del proceso SSO es muy limitada, ya que esta al llevarse a cabo desde el cliente se debe efectuar por el usuario, por lo cual las empresas deben tomar medidas adicionales de seguridad informática y control de acceso sobre los recursos.
- La administración llevada a cabo en cada una de las máquinas también provoca que las organizaciones deban realizar la configuración del SSO en cada una de las máquinas, lo cual hace esta tarea más lenta.

- El acceso de los usuarios a las aplicaciones desde diferentes computadoras se ve imposibilitado debido a que las credenciales se encuentran almacenadas en una sola máquina.

2. Administración centralizada con almacenamiento local de credenciales.

Este modelo de arquitectura resuelve algunos inconvenientes que presentó el Password vault al brindar el componente de administración de manera centralizada, con lo cual solamente el Agente SSO y las credenciales permanecen en el cliente favoreciendo en el control y monitoreo del proceso de ingreso y eliminando la necesidad de configurar el SSO en cada uno de los clientes. Para esta configuración se requiere los clientes necesarios, el servidor de aplicaciones y un servidor central para efectuar la administración. "Ver Figura 2"

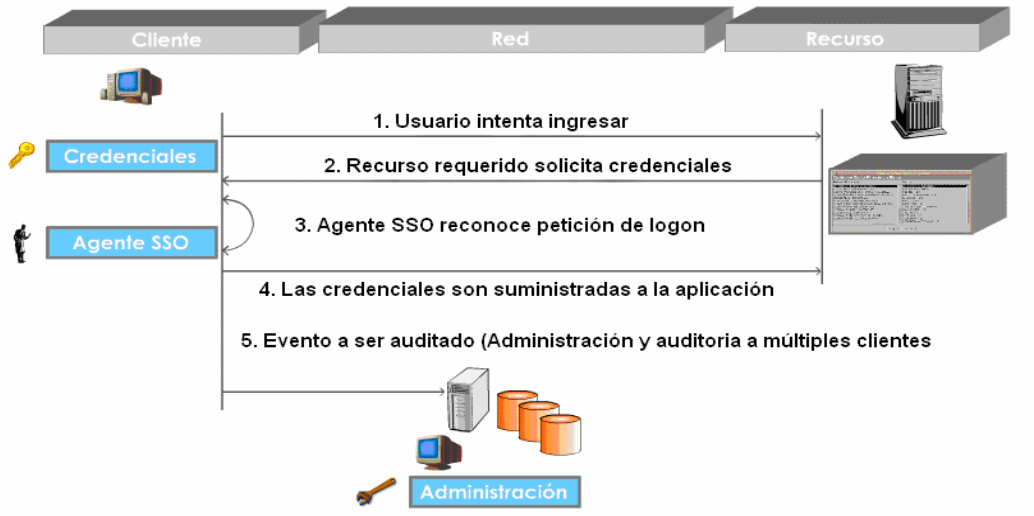

Figura 2

Fuente: http://www.criptored.upm.es/guiateoria/gt_m142j.htm

Ventaja

- Este diseño realiza la administración de manera centralizada por medio de un servidor central, el cual permite realizar las labores administrativas y llevar a cabo un control de la configuración y monitoreo del software del cliente con un bajo grado de complejidad.

Desventaja.

- Un inconveniente que presenta es que también al igual que la primer arquitectura presentada, almacena las credenciales en el cliente por lo que las empresas deben velar por definir medidas de control de acceso y confidencialidad de la información.

3. Administración y almacenamiento de credenciales centralizados.

Con este modelo de arquitectura, se intentan solucionar algunos problemas presentados con los diseños anteriores, controlando la administración y las credenciales de manera centralizada reduciendo controles de acceso de parte de la empresa. En este diseño un servidor central se encarga de realizar la administración además de tener almacenadas las credenciales, por lo que este servidor es indispensable además de los clientes y el servidor de aplicaciones. “Ver Figura 3”

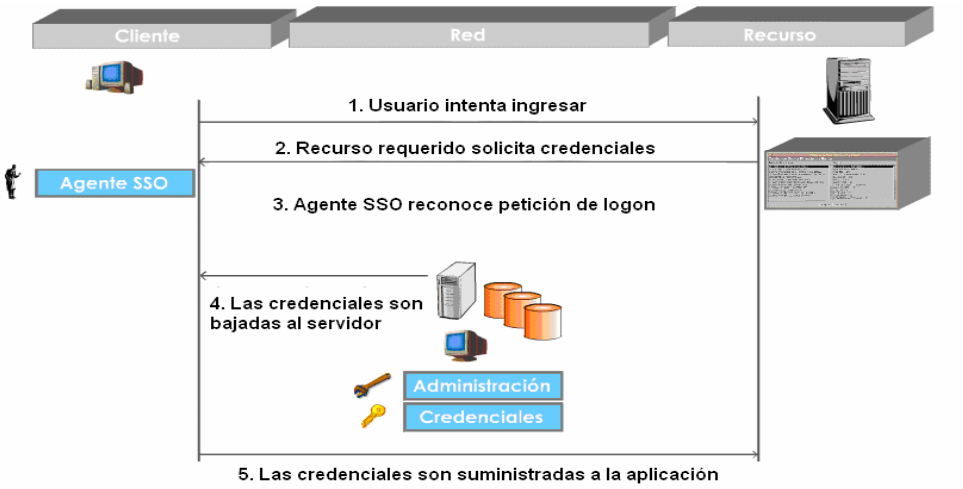

Figura 3

Fuente: http://www.criptored.upm.es/guiateoria/gt_m142j.htm

Ventajas.

- Al contar con las credenciales de cada uno de los usuarios para el acceso a las aplicaciones de una manera centralizada, brinda la posibilidad a estos de acceder a los recursos desde cualquier estación en la que se encuentren, con lo cual aumenta la disponibilidad de los recursos.
- Permite administrar adecuadamente las credenciales disminuyendo la manipulación de la misma desde los clientes y brindando un control sobre la frecuencia en que los usuarios solicitan las credenciales al servidor.

Desventajas.

- Se genera un único punto de falla ubicado en el servidor central, por lo que se toma un riesgo de perder información debido a que no se cuente con un respaldo en caso de presentarse algún problema.

- La configuración carece de redundancia y respaldos de la información.

4. Arquitectura SSO totalmente distribuida.

Esta es caracterizada por la separación del servidor y la base de datos con lo cual se superan algunos inconvenientes que pueden presentar los diseños anteriores, como la carencia de redundancia, recuperación entre fallas y respaldo. Para implementar este diseño además de poseer los clientes necesarios y el servidor de aplicaciones, se requieren múltiples servidores para brindar administración a los procesos y múltiples base de datos para el almacenamiento de las credenciales. "Ver Figura 4"

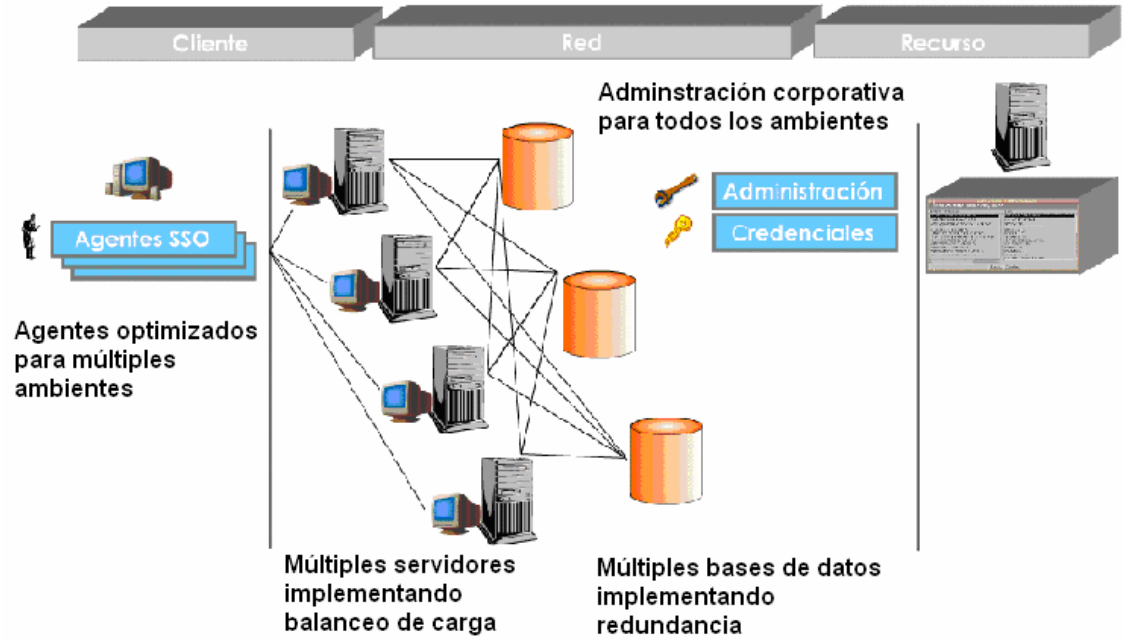

Figura 4

Fuente: http://www.criptored.upm.es/guiateoria/gt_m142j.htm

Ventajas.

- Posee múltiples bases de datos que se encuentran totalmente sincronizadas, con lo cual se logra la redundancia y el respaldo de la información.
- La información se almacena de manera encriptada, sin embargo hay que tomar en cuenta que cuando esta viaja entre un cliente SSO y el servidor, no va cifrada.
- El contar con varios servidores administrativos disminuye los riesgos que se tienen por amenaza de falla, balancea la carga con el aumento de la disponibilidad de información y el tiempo de respuesta hacia los clientes será menor.

Desventajas.

- La administración y el soporte se tornan más complejos debido a la cantidad de recursos que incluye su implementación.
- La implementación además es costosa debido a que requiere de recursos de alto costo y el implementarla técnicamente lleva mucho trabajo.

5. Administración y almacenamiento de credenciales centralizados garantizando alta disponibilidad y redundancia.

Este diseño se basa en administrar y almacenar las credenciales de manera centralizada y brindar algunos beneficios que presento el diseño anterior. En esta se requieren los clientes necesarios por la empresa, servidor y base de dato replicada para la redundancia y servidor de aplicaciones replicado como respaldo. “Ver Figura 5”

Figura 5

Fuente: http://www.criptored.upm.es/guiateoria/gt_m142j.htm

Ventajas.

- Cuenta con una réplica del servidor y base de datos central por lo que brinda redundancia de la información y permite a los usuarios conectarse desde varias estaciones.
- La disponibilidad de los recursos es mayor debido a que también posee una réplica del servidor de aplicaciones.

Desventajas.

- Presenta uno de los mayores limitantes en muchas empresas como lo es el costo de implementación, ya que este es alto debido a que tanto el hardware como el software deben estar debidamente respaldados.

Almacenamiento de credenciales

Como se describió y observó en las arquitecturas anteriores, el Agente SSO una vez que el usuario requiere acceder a una determinada aplicación, solicita la identificación correspondiente al componente Credenciales.

Las credenciales son almacenadas en repositorios centralizados en los casos en que no son almacenadas en las máquinas clientes, los cuales son bases de datos planas, no relacionales y son conocidos como directorios. De estos se obtiene la información requerida mediante un servicio de directorio.

Características del directorio:

- Son accedidas principalmente para lectura y búsqueda de la información.
- Soportan altos volúmenes de solicitudes de lectura.
- No permite realizar actualizaciones constantemente como se realiza en una base de datos relacional.
- No requiere de una estricta consistencia en la información.
- Se requiere de un protocolo de acceso tal como el DAP, LDAP, etc.

Un servicio de directorio es la fuente de la información del directorio y los servicios que hacen que la información este disponible a los usuarios. Este proporciona los medios para manejar correctamente el acceso a los recursos de un sistema de computadoras de red y además identifica a los usuarios y a los recursos de manera única sobre una red.

Funciones.

- Identificación y autenticación.
- Seguridad para los objetos.
- Replicar un directorio.
- Dividir un directorio.

Algunos servicios de directorio son:

- Directorio LDAP
- Active Directory
- Novell Directory Services
- iPlanet.
- OpenLDAP

Estructura del servicio directorio.

- Estructura lógica: objetos, atributos, clases, unidades de organización, dominios, árboles.
- Estructura Física.

Acceso a servicios de directorio.

El acceso del Agente SSO al servicio de directorio, es realizado mediante protocolos de acceso, los cuales son definidos mediante estándares creados sobre servicios de directorio.

El estándar X-500 es uno de ellos, el cual fue creado por Estándares Internacionales (ISO) y el Comité Consultivo Internacional de Telefonía y Telegrafía (CCITT) para servicios de directorio, el cual organiza la entrada de datos de forma jerárquica, permite almacenar grandes cantidades de información y realizar búsquedas constantes de la misma, entiéndase como entrada un objeto, persona, impresora o servidor. La comunicación entre el cliente y el servidor definida en este estándar debe ser mediante un protocolo de acceso como ya se mencionó, por lo que el X-500 utiliza el *DAP (Directory Access Protocol)* que pertenece a la capa superior de OSI.

Seguidamente del X-500 surge el estándar LDAP el cual se basa en el X-500, pero por supuesto con algunas mejoras y eliminando algunas opciones casi no utilizadas en este. El LDAP define la comunicación entre el cliente y el servidor con un protocolo *LDAP (Lightweight Directory Access Protocol)* que realiza la comunicación mediante TCP/IP y no mediante protocolos ISO como lo hace el X-500. El LDAP además de brindar más facilidad de implementación, requiere de menos recursos y es más comprensible.

Los servicios de directorio ya mencionados fueron implementados en LDAP, por lo que éste estándar puede ser utilizado para la implementación del Single Sign-On. Este permite mediante el protocolo LDAP de tipo cliente/servidor, realizar la comunicación entre los Agentes SSO y el servidor de directorio, permitiendo además y como una de sus mayores ventajas, realizar una comunicación desde diferentes plataformas.

Versiones LDAP:

- LDAP (RFC 1777 “Protocolo ligero de acceso a directorios”)
- LDAP v2
- LDAP v3 (RFC 2251 ” Protocolo ligero de acceso a directorios, versión 3”)

Comunicación entre cliente y servidor LDAP.

Cuando una aplicación requiere acceder a un directorio, esta no lo realiza directamente, para ello necesitará inicialmente llamar una función *API (application programming interface)* la cual origina un mensaje de acceso al directorio para ser enviado mediante el protocolo de acceso a otro proceso que se encarga de acceder el directorio y responder a la consulta realizada desde la aplicación. “Ver Figura 6”

Figura 6

Fuente: http://glud.udistrital.edu.co/glud/areas/doc/articulos/11_ldap/

Administración de la autorización.

Similar a la autenticación por parte del usuario, la administración de la autorización es llevada a cabo de forma centralizada, es decir, todos los permisos de acceso que poseen los usuarios para los diferentes recursos y plataformas que posee la empresa, serán almacenados y dirigidos desde una aplicación SSO, por parte de uno o varios administradores encargados.

Esta aplicación le va a permitir al administrador interactuar con el servidor de directorio en el cual podrá crear, modificar y eliminar las cuentas de los usuarios, así como también la asignación de los permisos de acceso para cada una de las cuentas y demás información personal del usuario.

El administrador encargado realizará la asignación de ciertos derechos de acceso sobre los respectivos recursos del sistema, basado en algunos de los siguientes datos del usuario:

- Roles o funciones a desempeñar dentro de la empresa.
- Ubicación física.
- Tipo de transacción.
- Grupo de pertenencia dentro de la empresa.
- Hora del día.

Toda esta información administrada, deberá ser de gran responsabilidad por parte del encargado, ya que de esta dependerán todos los recursos que la empresa posee para brindar el acceso al usuario que lo solicite o por el contrario no conceder el acceso.

Tipos de Single Sign-On

Existen dos tipos principales de SSO que pueden ser implementados basados en las arquitecturas descritas, estos tipos son el WEB-SSO que esta basado en WEB y E-SSO que se refiere a las aplicaciones legacy. Las aplicaciones legacy son sistemas de administración de base de datos (DBMSs) ejecutas desde mainframes o miniordenadores. Parte de las aplicaciones de la empresa, están clasificadas en estos dos tipos básicamente, por lo que se describirá un poco cada uno de éstos.

WEB Single Sign-On (W-SSO).

En el caso de la WEB, esta consta de portales de entrada para el usuario hacia varios sitios WEB, algunos de estos portales están dedicados a dar acceso a un servicio en específico, mientras que otros tratan de brindar el acceso a muchos servicios de la empresa. Estos portales brindan una interfaz al usuario mediante la cual estos pueden acceder a las WEB desde las cuales se da un enlace directo entre el usuario y la aplicación de la cual este desea obtener algún servicio.

Mediante el SSO se puede llevar a cabo la autenticación del usuario desde el portal WEB. El usuario se identifica en el portal WEB y el SSO valida los servicios WEB a los cuales tiene acceso, y una vez que el usuario opte por un servicio desde el portal, el SSO podrá autenticar al usuario automáticamente para poder accederlo.

Enterprise Single Sign-On (E-SSO).

El E-SSO no está basado en WEB, pero utilizan la misma arquitectura de autorización y autenticación de W-SSO exceptuando que no cuentan con un portal para facilitar el acceso a varias aplicaciones. Los legacy Single Sign-On permiten ingresar a varias aplicaciones desde la Intranet de la organización a través de una autenticación. Similar al W-SSO, luego de una autenticación inicial se validan los requerimientos de las aplicaciones secundarias para autenticar al usuario en la aplicación que desee utilizar.

Ventajas del SSO.

Aumento de productividad.

La productividad del usuario en beneficio de la empresa se ve mejorada, ya que el tiempo que se tarda en brindar los permisos de acceso a todas las aplicaciones que requerirá el usuario, disminuiría notablemente por el hecho de solo tener que facilitar una identificación a este. Este tiempo antes perdido puede ser mejor aprovechado por el usuario.

Además, los recursos del *help desk* utilizados para restablecer las contraseñas, pueden ser asignados a otros proyectos, debido a que con la utilización de solo una identificación por parte del usuario, habrá menos probabilidad de olvidarla.

Facilidad de acceso a recursos.

Permite el acceso de los usuarios desde varias plataformas a las diferentes aplicaciones a las cuales tiene permiso en un menor tiempo.

Administración sencilla de credenciales.

El aprovisionamiento, mantenimiento y eliminación de las credenciales del usuario llevado a cabo por el administrador, es mucho más sencillo debido a que SSO administra las credenciales y demás información de manera centralizada con la utilización de un servicio directorio.

Aumento de seguridad.

La seguridad aumenta con el SSO, ya que el usuario al utilizar solamente una identificación para el ingreso, no se ve obligado a escribir en un documento las contraseñas para poder recordarlas como sucede a veces, con lo cual podría exponerlas a individuos no permitidos.

El SSO además brinda la facilidad de adaptar procesos de autenticación fuerte, esto se debe a que dicho proceso solamente se realiza una vez con lo cual se accede a todos los recursos, por lo que si no se le da un control adecuado, cualquier persona que obtenga la contraseña podría acceder a todos los servicios asociados a la cuenta. La autenticación fuerte se refiere al proceso de autenticación en sistemas que requieren múltiples factores para realizar la identificación del usuario, los cuales utilizan tecnología avanzada como contraseñas dinámicas, certificados digitales, *biometric,* reconocimiento de voz, etc. Un ejemplo son las tarjetas de débito, las cuales además de requerir la tarjeta, se requiere de una clave para acceder y realizar las transacciones.

Desventajas del SSO.

Punto de falla centralizado.

Debido a que la autenticación inicial llevada a cabo por medio del Single Sign-On para la validación del usuario, se realiza mediante un solo proceso, se crea un punto de falla único, ya que si este proceso falla, sea por fallo en el servidor de aplicaciones, fallo en el servidor de credenciales o fallo en el agente SSO podría afectar todo el proceso y no permitir al usuario realizar sus labores.

Acoplamiento con Sistemas Operativos.

A pesar de que Single Sign-On contempla gran variedad de ambientes de sistemas operativos desde los cuales se puede acceder a las aplicaciones, otros ambientes quedan por fuera de este proceso, y algunos requieren de herramientas adicionales para poder ser parte del proceso, lo cual para algunas empresas dificulta la implementación ya que utilizan diferentes sistemas operativos.

Herramientas para fortalecimiento de Seguridad.

Como se mencionó en las ventajas del SSO, este permite adicionar procesos de autenticación fuerte con el fin de aumentar la seguridad, pero cabe resaltar que estos procesos no son parte de una solución Single Sign-On, por lo que toda empresa que requiera robustecer el proceso de autenticación requerirá de recursos adicionales para implementarlo.

Costos de implementación.

Los costos asociados con el desarrollo de un SSO pueden ser significativos cuando se considera la naturaleza y extensión de las interfaces a ser desarrolladas y mantenidas, como se indicó anteriormente, existen varias arquitecturas que pueden ser implementadas, por lo que el costo varía para cada una de ellas pero de igual forma estas requerirán de gastos de adquisición de hardware y de software considerables.

Productos en el mercado.

Productos Líderes	
Vendedor	Nombre del producto
Axent Technologies (www.axent.com)	Enterprise Resource Manager
Bull (www.bull.com)	Access Master
CKS (www.cksweb.com)	My Net
Computer Associates Inc. (www.cai.com)	Platinum Family
iT SEC	iT Secure Sign On
Unisys (www.unisys.com)	Single Point Security

Tabla 1.

Productos Desafiadores	
Vendedor	Nombre del producto
Century Analysis Inc. (www.cainc.com)	CAI-Net
Computer Associates International	Unicenter SSO
Cyber Safe (www.cybersafe.com)	Trust Broker - Security Suite And Defensor
Hewlett-Packard (www.hp.com)	Praesidium SSO
IBM (www.ibm.com)	Global Sign-On
Proginet (www.proginet.com)	SecurPass
RSA Security (www.rsasecurity.com)	Boks SSO/SecurSight Manager
Softools (www.softools.fr)	SoftSSO

Tabla 2.

Conclusiones.

1. Ante lo indispensable que se torna el contar con métodos para fortalecer la seguridad contra las amenazas que aumentan día con día en las empresas, y debido a la situación ya presentada con la descentralizada y desorganizada administración de la autenticación que dificulta la labor tanto del administrador como la de los usuarios, el Single Sign-On ofrece el apoyo necesario a todo este proceso de administración, el cual surge como una de las soluciones mas viables y beneficiosas a implementar en una organización.

   Las empresas que deseen reforzar el sistema contra individuos no deseados y brindar una mayor facilidad de acceso de los usuarios a los recursos que poseen, tienen grandes posibilidades de alcanzarlo con un producto Single Sign-On, ya que este brinda la opción de implementar alguno de los diferentes diseños SSO, dependiendo de las características de la organización y de sus recursos disponibles brindando resultados similares.

2. El Single Sign-On puede ser implementado en cinco diferentes arquitecturas posibles, pero en base a las características mostradas para cada uno de los diseños, el que se puede adaptar con mayor facilidad tomando en cuenta los recursos de cómputo y los recursos económicos con los que cuentan la mayoría de organizaciones, es el diseño que lleva a cabo la administración y el almacenamiento

de credenciales de manera centralizada, ya que brinda el servicio SSO con un control debido de las identidades de los usuarios y el proceso SSO, con pocos recursos de cómputo, por lo que su costo de implementación no es tan alto.

Claro está, que si se cuenta con el recurso económico suficiente sería totalmente adecuado implementar la arquitectura SSO totalmente distribuida que brinda mucho más beneficios.

3. El SSO a pesar de poseer algunas desventajas ya mencionadas, logra solucionar algunas con el apoyo de herramientas adicionales o algunas soluciones que pueden ser adaptadas, además de que con respecto a las ventajas que brinda esta solución, la empresa más que verse afectada, soluciona una variedad de inconvenientes presentados actualmente.

   Estas soluciones están haciendo que surjan gran variedad de competidores que brindan una solución SSO, que al mirar la necesidad de las empresas por implementar este tipo de soluciones se han dado a la tarea de introducir en el mercado nuevos productos que con el paso del tiempo pueden tomar mayor fuerza e interés por parte de las organizaciones.

Bibliografía.

Artículos en Internet.

Jacqueline Emigh. (2005). Single Sign-On, Multiples Benefits. Recuperado el 15 de Octubre del 2005, de http://govtsecurity.com/mag/single_signon_multiple/

Jeimy J. Cano, Iván M. Caballero. (2003). Consideraciones para Implementar una Arquitectura Single Sign-On. Recuperado el 06 de Noviembre del 2005, de http://www.criptored.upm.es/guiateoria/gt_m142j.htm

Jeremy Smith's. (2005). The Benefits of Single Sign On. Recuperado el 16 de Octubre del 2005, de http://blog.case.edu/jms18/2005/06/27/the_benefits_of_single_sign_on

John Becerra, Mauricio Galindo. (2003). LDAP. Recuperado el 13 de Noviembre del 2005, de http://glud.udistrital.edu.co/glud/areas/doc/articulos/11_ldap/

Laura Taylor. (2002). Understanding Single Sign-On. Recuperado el 06 de Noviembre del 2005, de http://www.intranetjournal.com/articles/200205/se_05_28_02a.html

Michael Donnelly. (2000). Una Introducción a LDAP. Recuperado el 15 de Noviembre del 2005, de http://ldapman.org/articles/sp_intro.html

Páginas en Internet.

BIONETRIX. (2002). Enterprise Single Sign-On: Balancing Security & Productivity. Recuperado el 06 de Octubre del 2005, de http://www.cs.plu.edu/courses/CompSec/arts/sso.pdf

Java en Castellano. (1999). Introducción al X.500. Recuperado el 15 de Noviembre del 2005, de http://www.programacion.com/java/tutorial/jndi2/3/

M-TECH: Identity Management Solutions. (2005) Definition of Single Sign-On. Recuperado el 06 de Octubre del 2005, de http://mtechit.com/concepts/single_sign_on.html

Netigy Corporation. (2000). Single Sign-On: Myth or Reality. Recuperado el 06 de Octubre del 2005, de http://csrc.ncsl.nist.gov/nissc/2000/proceedings/papers/303slide.pdf

PassGo Technologies. (2005). Single Sign-On Solutions. Recuperado el 02 de Noviembre del 2005, de http://www.passgo.com/products/sso/index.shtml

TechTarget Security Media. (2003). Definitions Single Sign-On. Recuperado el 06 de Octubre del 2005, de http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci340859,00.html