

SISTEMA CENTRALIZADO DE AUTENTICACIÓN Y AUTORIZACIÓN
“SINGLE SIGN ON”

Documento Final de Trabajo de Grado
Modalidad Pasantía

LAURA ESTEFANÍA GÁLVEZ VIDALES
1056282
lauraestefania@gmail.com

Universidad del Valle
Programa Académico de Ingeniería de Sistemas
Noviembre de 2013

SISTEMA CENTRALIZADO DE AUTENTICACIÓN Y AUTORIZACIÓN
“SINGLE SIGN ON”
Documento Final de Trabajo de Grado
Modalidad Pasantía

LAURA ESTEFANÍA GÁLVEZ VIDALES
1056282
lauraestefania@gmail.com

Trabajo de grado para optar el título de Ingeniero de Sistemas

Director:
Ing. Carlos A. Laverde Figueroa
Gerente Línea Infraestructura

Codirector:
Ph.D. Angel García Baños
Director Escuela de Ingeniería de Sistemas y Computación

Universidad del Valle
Programa Académico de Ingeniería de Sistemas
Noviembre de 2013

Nota de aceptación

Presidente del Jurado

Jurado 1

Jurado 2

Tuluá, Noviembre de 2013

Dedicatoria

Este trabajo va dedicado a las personas que me apoyaron en todo el proceso, en especial a mi papá, mi mamá, mis hermanos, mi compañero y mis amigas incondicionales que siempre me dieron ánimos en el camino.

Agradecimientos

Un profundo agradecimiento a los profesores que a lo largo de mi carrera han impartido su conocimiento, mi director Ángel Baños que me apoyó en todo el proceso y confió en mí para realizar este trabajo.

A la empresa Carvajal Tecnología y Servicios que me permitió realizar esta pasantía, brindando todo lo necesario para llevarla a cabo y culminarla con éxito, aportando una excelente experiencia laboral.

A mi jefe Carlos Laverde quien desde el principio me brindó su confianza, apoyo y que vio en mí el potencial para sacar adelante este proyecto.

A mis compañeros laborales que con su alegría, entusiasmo y apoyo hicieron de esta experiencia algo único.

A mis compañeros de estudio que durante el proceso me dieron ánimo y por su compañía en estos años donde definitivamente se crearon lazos de amistad.

A mi familia que siempre ha estado a mi lado, me aconsejaron y acompañaron en cada paso que tuve a través de mi carrera.

Contenido

1. Introducción.....	13
1.1 Descripción general.....	13
1.2 Problema.....	14
1.2.1 Descripción del problema.....	14
1.2.2 Formulación del problema.....	14
1.3 Objetivos.....	15
1.3.1 General.....	15
1.3.2 Específicos.....	15
1.4 Estructura del documento.....	15
2. Marco referencial.....	16
2.1 Marco conceptual.....	16
2.2 Antecedentes.....	19
3. Desarrollo del proyecto.....	22
3.1 Análisis.....	22
3.1.1 Especificación de requerimientos.....	22
3.1.2 Historias de usuario.....	23
3.2 Diseño.....	24
3.2.1 Arquitectura.....	24
3.2.1.1 Metapass SSO.....	24
3.2.1.2 E-SSOM.....	25
3.2.2 Directorio Activo.....	29
3.2.3 Base de Datos.....	36
3.2.3.1 Metapass SSO.....	36
3.2.3.2 E-SSOM.....	40
3.3 Implementación.....	41
3.3.1 Metapass SSO.....	41
3.3.2 E-SSOM.....	45
3.4 Pruebas.....	48
3.4.1 Pruebas de usabilidad.....	48
3.4.2 Pruebas alfa y beta.....	52
4. Conclusiones.....	54
Referencias.....	55

Lista de tablas

Tabla 1.1 Relación objetivos específicos con los resultados esperados.....	15
Tabla 3.1 Requerimientos funcionales, módulo de usuarios.....	22
Tabla 3.2 Historias de usuario.....	23
Tabla 3.4 Caso de estudio, pruebas de usabilidad E-SSOM.....	48
Tabla 3.5 Caso de estudio, pruebas de usabilidad Metapass SSO.....	49

Lista de figuras

Figura 3.2 Arquitectura Metapass SSO.....	24
Figura 3.3 Arquitectura E-SSOM.....	25
Figura 3.4 Central Service.....	26
Figura 3.5 Múltiples servicios centrales.....	27
Figura 3.6 Múltiples bases de datos.....	27
Figura 3.7 User Client GUI.....	28
Figura 3.8 Replicación de directorio.....	30
Figura 3.9 Estructura lógica del AD.....	31
Figura 3.10 Árbol de dominio.....	32
Figura 3.11 Tecnologías de Active Directory.....	33
Figura 3.12 Estructura general (OU).....	34
Figura 3.13 OU usuarios.....	34
Figura 3.14 Propiedades usuarios.....	35
Figura 3.15 Autenticación Windows.....	36
Figura 3.16 Contraseña maestra.....	36
Figura 3.17 KIOSK.....	37
Figura 3.18 DPAPI es una API.....	38
Figura 3.19 Relación de claves.....	39
Figura 3.20 Arquitectura del cifrado TDE.....	41
Figura 3.21 Conexión servidor-directorio activo.....	43
Figura 3.22 Carga de usuarios administrativos.....	43
Figura 3.23 Carga de usuarios técnicos informáticos.....	43
Figura 3.24 Creación flujo de trabajo.....	44
Figura 3.25 Aplicaciones para un grupo (OU).....	44
Figura 3.26 Desktop SSO.....	45
Figura 3.27 Consola de administración.....	46
Figura 3.28 Aplicaciones.....	46
Figura 3.29 Ícono “objetivo” para realizar la virtualización.....	47
Figura 3.30 Cliente usuarios finales.....	47

Lista de gráficos

Gráfico 3.4 Proceso de ingreso a las aplicaciones.....	50
Gráfico 3.5 Percepción del software.....	50
Gráfico 3.6 Necesidad de ayuda técnica.....	51
Gráfico 3.7 Encontrar las funcionalidades requeridas.....	51
Gráfico 3.8 Proceso para cambiar credenciales.....	52

Lista de anexos

Anexo A: Especificación de requerimientos
Anexo B: Guía de instalación Metapass SSO
Anexo C: Guía de instalación E-SSOM

Resumen

El principal objetivo de una arquitectura SSO (Single Sign On) es transferir la funcionalidad de autenticación propia de cada programa a un solo servicio de SSO.

En una arquitectura SSO, todos los mecanismos de seguridad se encuentran concentrados en el SSO, siendo éste el único punto de autenticación en el sistema.

Otro beneficio de una arquitectura Single Sign On es que los usuarios deben hacer el proceso de ingreso una sola vez a cada aplicación, a pesar de que continúan interactuando con múltiples componentes de seguridad en el sistema.

El concepto Single Sign On no necesariamente se refiere a una sincronización de contraseñas, ya que en ese caso todas las aplicaciones y servicios funcionarían con una misma contraseña, pero no es una buena solución, ya que en lugar de fortalecer la seguridad, la estaría debilitando.

Una implementación real de SSO, deberá contar con un agente SSO que se encarga de almacenar en una base de datos o directorio protegido los passwords que le permiten al usuario acceder a cada una de las aplicaciones o servicios, en el momento que lo desee, ya que el proceso de login se realiza de manera transparente al usuario, una vez que éste ha sido autenticado por medio de una arquitectura SSO.

Palabras clave: single sign on, autenticación, login, sso, arquitectura sso

Abstract

The main objective of a SSO architecture (Single Sign On) is to transfer the functionality of authentication of every program to a single SSO service.

In a SSO architecture, every security mechanisms are concentrated on the SSO, as the system's only authentication point.

Another advantage of an SSO architecture is that the users must log in only once to each application even while they interact with multiple system's security components.

The SSO concept does not necessarily means password synchronization, in that case every application and service would work with the same password but that is not a good solution, since instead of enhancing security it is making it weaker.

A real SSO implementation must count with an SSO agent which stores passwords in a database or a protected path, granting users access to every application and service anytime they want, since the login occurs in a transparent way to them, once they have been identified by an SSO architecture.

Keywords: single sign on, authentication, login, sso, architecture sso

Capítulo 1

Introducción

1.1 Descripción general

En la empresa Carvajal S.A. actualmente hay cerca de 16000 empleados que hacen uso de las diferentes aplicaciones que tienen en la compañía, según *Carlos Laverde*¹. Al existir tantas aplicaciones, los empleados deben recordar diferentes usuarios y contraseñas para cada una de ellas, dónde el constante olvido de contraseñas genera altos costos de administración, situación que ocasiona la generación de contraseñas inseguras por parte de los usuarios finales “para que no sean olvidadas”, lo que evidentemente no se logra, incrementando así las posibilidades de vulnerabilidad de los sistemas.

Por lo tanto, se propone implementar una aplicación para controlar la autenticación de los sistemas informáticos de la empresa Carvajal S.A., para brindar acceso a todas las aplicaciones con solo una instancia de verificación, que permita disminuir el número de peticiones a la mesa de ayuda, reducir los costos de administración y seguridad en la empresa.

¹ Carlos Laverde es Gerente Línea Infraestructura en Carvajal Tecnología y Servicios

1.2 Problema

1.2.1 Descripción del problema

Actualmente la empresa Carvajal S.A. cuenta con alrededor de 16000 usuarios que hacen uso de las diferentes aplicaciones que la empresa posee, siendo aproximadamente 27 aplicaciones (Web y Desktop), dónde en cada una de éstas, cada usuario ingresa con sus datos de autenticación para iniciar una sesión determinada. Ahora bien, un usuario para cada aplicación, tiene diferentes datos de autenticación, dado que dichos datos reposan en cada aplicación con estructuras, condiciones, políticas y estándares que cada una defina.

Se evidencia la dificultad que los usuarios en la empresa tienen conflictos a la hora de autenticarse por diferentes razones, al tener varios nombres de usuario y diferentes contraseñas el usuario puede olvidar, o equivocarse al ingresar los datos lo cual genera pérdida de tiempo, reduciendo eventualmente la productividad.

El usuario se remite a una mesa de ayuda, cuya función en la empresa es solucionar problemas a los usuarios, supliendo la necesidad del empleado al olvidar sus datos para autenticarse.

La mesa de ayuda de Carvajal S.A. recibe en promedio 10000 llamadas al mes, de estas 10000 llamadas, entre el 20% y 25% es de cambio de contraseñas de todas las aplicaciones.

Al ser tantos usuarios que presentan esta problemática, esto se ve reflejado en la gran cantidad de llamadas a la mesa de ayuda, según Carlos Laverde, ocasionando una gran pérdida de tiempo, ya que los usuarios pausan sus actividades mientras esperan la pronta solución, esto genera ineficiencia al no poder continuar sus procesos a tiempo, además no resuelve el problema de raíz, siendo tratados los problemas de manera temporal y superficial.

También es de suma importancia para la empresa aumentar la seguridad, ya que la integridad de la información es lo más importante a tener en cuenta para cualquier organización.

Se hace indispensable darle solución a esta problemática, para así disminuir la operatividad asociada con la administración de contraseñas, poder aumentar la seguridad, reducir peticiones a la mesa de ayuda, reducir los altos costos de administración que generan estas peticiones y aumentar la productividad. Por lo tanto es necesario pensar en una solución que permita la implementación de contraseñas seguras que sirvan para todos los sistemas sin necesidad de digitarlas cada vez que se requiera accesibilidad.

1.2.2 Formulación del problema

¿Qué debe tener un sistema de autenticación y autorización de usuarios y contraseñas que deba tener la empresa Carvajal S.A.; permitiendo disminuir el número de peticiones a la mesa de ayuda, reducir los costos de administración, y aumentar la seguridad?

1.3 Objetivos

1.3.1 Objetivo general

Controlar la autenticación de los sistemas de información de la empresa Carvajal S.A, para brindar acceso a todas las aplicaciones con solo una instancia de verificación, que permita disminuir el número de peticiones a la mesa de ayuda, reducir los costos de administración y aumentar la seguridad en la empresa Carvajal S.A.

1.3.2 Objetivos específicos

En la tabla 1.1 se relacionan los objetivos específicos con la sección de este documento que expone el resultado de cada objetivo propuesto.

OBJETIVO ESPECÍFICO	SECCIÓN
1. Determinar el tipo de arquitectura Single Sign On que se adecúe mejor a la organización, de acuerdo a la realidad tecnológica que se tenga, permitiendo la conexión a las diferentes aplicaciones con una sola instancia de autenticación en cada aplicación, facilitando las tareas de administración.	3.2.1
2. Configurar el directorio activo de Microsoft de la compañía, para garantizar el inicio de sesión de las cuentas de la empresa que se encuentran registradas.	3.3
3. Garantizar el acceso al correo institucional, sincronizado con las demás aplicaciones a las que se tengan privilegios.	3.3

Tabla 1.1: Relación objetivos específicos con los resultados esperados

1.4 Estructura del documento

El resto del documento está organizado de la siguiente manera:

En el *capítulo 2: Marco Referencial*, se presenta el marco conceptual y los antecedentes acerca de Single Sign On.

En el *capítulo 3: Desarrollo del proyecto*, se presenta el proceso de documentación, diseño y tecnologías utilizadas a lo largo del desarrollo del proyecto, llevados a cabo para cumplir con los objetivos propuestos, así como los diferentes modelos de pruebas que se realizaron.

Este trabajo finaliza con el *capítulo 4: Conclusiones*.

Capítulo 2

Marco Referencial

En el presente capítulo se definen los conceptos usados y discutidos en el trabajo de grado y durante el proceso de práctica. Además se exponen los antecedentes en el área de los sistemas centralizados de autenticación y autorización.

2.1 Marco conceptual

Mesa de Ayuda

También llamada *Help Desk*², es un conjunto de servicios que ofrece la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las TICs, siendo un área específica de la empresa a la cual se comunican los usuarios por medio de llamadas telefónicas cuando tienen inconvenientes relacionados con software o hardware, siendo la mesa de ayuda la que soluciona estos problemas en primera instancia.

TICs

Las tecnologías de la información y la comunicación TICs³, agrupan los elementos y las técnicas usadas en el tratamiento y la transmisión de la información, principalmente la informática, Internet y las telecomunicaciones.

Autenticación

Es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. En un web de confianza, "autenticación"⁴ es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacerlo.

Autorización⁴

Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.

Administración de usuarios

Perfiles de los usuarios, permisos a cada usuario, a que aplicaciones pueden acceder y que pueden hacer dentro del sistema.

Algoritmos de encriptación⁵

Un algoritmo criptográfico, o cifrador, es una función matemática usada en los procesos de encriptación y desencriptación. Un algoritmo criptográfico trabaja en

² http://es.wikipedia.org/wiki/Mesa_de_ayuda

³ http://gtea.uma.es/congresos/CDROM/comunicaciones/carpeta1/Comunicacion_SanchezVega_Elena-1.pdf

⁴ <http://es.wikipedia.org/wiki/Autenticaci%C3%B3n>

⁵ <http://www.cryptoforge.com.ar/seguridad.htm>

combinación con una llave (un número, palabra, frase, o contraseña) para encriptar y desencriptar datos. Para encriptar, el algoritmo combina matemáticamente la información a proteger con una llave provista. El resultado de este cálculo son los datos encriptados. Para desencriptar, el algoritmo hace un cálculo combinando los datos encriptados con una llave provista, siendo el resultado de esta combinación los datos desencriptados (exactamente igual a como estaban antes de ser encriptados si se usó la misma llave). Si la llave o los datos son modificados el algoritmo produce un resultado diferente. El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la llave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada llave posible. Incluso para una llave de sólo 40 bits, esto significa 2^{40} (poco más de 1 trillón) de llaves posibles.

Los algoritmos simétricos encriptan y desencriptan con la misma llave. Las principales ventajas de los algoritmos simétricos son su seguridad y su velocidad. Los algoritmos asimétricos encriptan y desencriptan con diferentes llaves. Los datos se encriptan con una llave pública y se desencriptan con una privada, siendo ésta su principal ventaja. Los algoritmos asimétricos, también conocidos como algoritmos de llave pública, necesitan al menos una llave de 3.000 bits para alcanzar un nivel de seguridad similar al de uno simétrico de 128 bits. Y son increíblemente lentos, tanto que no pueden ser utilizados para encriptar grandes cantidades de información. Los algoritmos simétricos son aproximadamente 1.000 veces más rápidos que los asimétricos.

RSA

El sistema criptográfico con clave pública RSA⁶ es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario, fue desarrollado en 1977 por Rivest, Shamir y Adleman.

La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10^{200} , y se prevé que su tamaño crezca con el aumento de la capacidad de cálculo de los ordenadores.

Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

JAVA⁷

Es un lenguaje de programación y la primera plataforma informática creada por *Sun Microsystems* en 1995. Es la tecnología subyacente que permite el uso de programas punteros, como herramientas, juegos y aplicaciones de negocios. Es un lenguaje de programación de propósito general, concurrente, orientado a objetos y basado en

⁶ <http://es.wikipedia.org/wiki/RSA>

⁷ <http://www.java.com>

clases que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible.

XML

*Extensible Markup Language*⁸ (lenguaje de marcas extensible), desarrollado por el *World Wide Web Consortium (W3C)* utilizado para almacenar datos en forma legible. Deriva del lenguaje SGML y permite definir la gramática de lenguajes específicos para estructurar documentos grandes. A diferencia de otros lenguajes, XML da soporte a bases de datos, siendo útil cuando varias aplicaciones se deben comunicar entre sí o integrar información.

XML no ha nacido sólo para su aplicación en internet, sino que se propone como un estándar para el intercambio de información estructurada entre diferentes plataformas. Se puede usar en bases de datos, editores de texto, hojas de cálculo y casi cualquier cosa imaginable.

XML es una tecnología sencilla que tiene a su alrededor otras que la complementan y la hacen mucho más grande y con unas posibilidades mucho mayores. Tiene un papel muy importante en la actualidad ya que permite la compatibilidad entre sistemas para compartir la información de una manera segura, fiable y fácil.

Arquitectura

En los inicios de la informática, la programación se consideraba un arte y se desarrollaba como tal, debido a la dificultad que entrañaba para la mayoría de las personas, pero con el tiempo se han ido descubriendo y desarrollando formas y guías generales, con base a las cuales se puedan resolver los problemas. A estas, se les ha denominado Arquitectura de Software, porque, a semejanza de los planos de un edificio o construcción, estas indican la estructura, funcionamiento e interacción entre las partes del software. La arquitectura es un nivel de diseño que hace foco en aspectos *"más allá de los algoritmos y estructuras de datos de la computación, el diseño y especificación de la estructura global del sistema es un nuevo tipo de problema"* [1].

Existen diferentes tipos de arquitecturas que permiten implementar SSO. Cada una de ellas posee características que las hace más apropiadas para algún tipo de organización. La decisión de adoptar una u otra arquitectura básicamente depende de los recursos computacionales y/o económicos disponibles y las decisiones de diseño establecidas por el equipo del proyecto.

Las diferentes *arquitecturas SSO* [3] están compuestas por tres componentes básicos:

- **Interfaz:** El modo en que el SSO interactúa con una determinada aplicación. Usualmente reside en el cliente y es conocido como agente SSO.
- **Administración:** El mecanismo que permite configurar, mantener y monitorear el proceso de SSO.
- **Credenciales:** Cada aplicación a la que se accede requiere información confidencial (nombre de usuario, contraseña, entre otras), que agrupada recibe el nombre de credenciales. Las credenciales deben almacenarse de manera protegida para que sea únicamente el agente SSO quien pueda acceder a ellas.

⁸ http://es.wikipedia.org/wiki/Extensible_Markup_Language y <http://www.w3.org/TR/REC-xml/>

Directorio Activo

El *directorío activo* [2], es un servicio de directorio. El término servicio de directorio se refiere a dos cosas; un directorio donde la información sobre usuarios y recursos está almacenada y donde un servicio o servicios dejan acceder y manipular estos recursos. El directorio activo es una manera de manejar todos los elementos de una red, incluidos ordenadores, grupos, usuarios, dominios, políticas de seguridad y cualquier tipo de objeto definidos para el usuario. Además de esto, provee funciones adicionales más allá de estas herramientas y servicios.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Single Sign On

El concepto de *Single Sign On* [3], se refiere al acceso a múltiples recursos por medio de un único proceso de ingreso. Gran cantidad de las arquitecturas implementadas en diferentes organizaciones han sido diseñadas con el objeto de dar acceso a los usuarios a múltiples servicios web y/o aplicaciones. En la mayoría de los casos se encuentra que cada uno de los servicios o aplicaciones cuenta con su propio componente de seguridad, lo cual generalmente compromete la seguridad de todo el sistema, dado que el nivel de seguridad de todo un sistema es igual al nivel de seguridad del componente más inseguro que lo compone. Una de las posibles soluciones a este problema es implementar la estrategia *Single Sign On*.

El principal objetivo de una arquitectura que implemente *Single Sign On* es transferir la funcionalidad y complejidad de todos los componentes de seguridad a un solo servicio de *Single Sign On* (SSO). En una arquitectura SSO, todos los mecanismos de seguridad se encuentran concentrados en el SSO, siendo éste el único punto de autenticación y registro en el sistema. Otro beneficio de una arquitectura *Single Sign On* es que los usuarios deben hacer el proceso de ingreso una sola vez.

2.2 Antecedentes

- **Kerberos**

Kerberos [4], permite a dos computadores de una red insegura demostrar su identidad mutuamente de manera segura, es un modelo cliente-servidor y brinda autenticación mutua. Se basa en criptografía de clave asimétrica y requiere un tercero de confianza; utiliza el protocolo de Needham-Schroeder y el tercero de confianza es denominado como “centro de distribución de claves” y consiste en dos partes lógicas separadas: un “servidor de autenticación” y un “servidor emisor de tickets”. Los “tickets” sirven para demostrar la identidad de los usuarios. No fue posible implementarlo, ya que para hacerlo es necesario cambiar parte de las aplicaciones para integrarlas a kerberos.

- **Visual Guard**
Visual Guard [5], principalmente ofrece un directorio activo para las aplicaciones de la empresa el cual permite autenticación y autorización, definir permisos para cada cuenta y permite además el sistema de autenticación única (SSO). Pero es solo para aplicaciones .Net, por lo tanto no es posible, ya que las diferentes aplicaciones de la empresa están bajo distintos lenguajes de programación.
- **OneSign**
One Sign [6], la aplicación simplifica el conectarse y desconectarse, automatizando nombre de usuario y contraseña de entrada para los usuarios autenticados. Probado en entornos de salud, puede usarse con aplicaciones clínicas, financieras y administrativas, ahorrando tiempo significativo en proveedores de atención y mejorando la satisfacción, no es necesario instalar software adicional.
- **ESSO Suite**
El *Oracle Enterprise Single Sign On Suite* [7], ofrece una alta adaptabilidad y una infraestructura administrativa de identidad corporativa escalable, que provee características como autenticación fuerte, provisionamiento de credenciales centralizadas para la mayoría de aplicaciones Windows, Web, Java y cambio de contraseña en las aplicaciones, entre otros.
- **Google**
Unifica sus servicios bajo una única cuenta de usuario (gmail, google+, youtube, google docs, entre otras), una vez que se accede a alguna de ellas, puedes acceder a cualquiera de sus otros servicios sin la necesidad de autenticarse otra vez.
- **AccessMaster Single Sign On**
Evidian Enterprise SSO [8], software de inicio único de sesión, ingresa las contraseñas de las aplicaciones automáticamente, en lugar del usuario, y se pueden cambiar las contraseñas de acuerdo a políticas estrictas. Esto garantiza la seguridad de acceso a las aplicaciones, manteniendo las tareas sencillas para los usuarios y los administradores. No se necesita modificar ninguna de las aplicaciones, disponible para aplicaciones web, cliente/servidor, SAP. Basado en directorio LDAP o directorio activo.
- **Crowd (Atlassian)**
Crowd: Identity management for web apps [9], es una herramienta Single Sign On web que simplifica la gestión de identidades. Los administradores pueden manejar la autenticación y la autorización para los usuarios, aplicaciones web, servidores de directorio tanto como sean necesarios, todo a través de una sola interfaz intuitiva.
- **PingFederate**
PingFederate [10], realiza tres funciones críticas de seguridad que hacen que el acceso a las aplicaciones de Internet sea más fácil y más seguro: Internet Single Sign-On, Internet Gestión de cuentas de usuario, y Universal Token Traducción. Los usuarios se registran una vez a su red corporativa, a continuación, PingFederate comunica de forma segura sus identidades Web-based/Cloud a las aplicaciones internas y externas. No son necesarias contraseñas individuales de las aplicaciones y no se requieren logueos adicionales, aumentando la comodidad del usuario y haciendo las aplicaciones más seguras. PingFederate también se integra con el

directorio corporativo de forma automática para crear, actualizar y desactivar cuentas de usuario para las aplicaciones de Internet en todo el ciclo de vida del usuario. Cuando un usuario sale de la organización o ya no requiere acceso a las aplicaciones, PingFederate desactiva inmediatamente la cuenta de ese usuario en la aplicación de Internet, lo que garantiza que sólo los usuarios autorizados tienen acceso a la aplicación. El servicio de token de seguridad de PingFederate traduce los tokens de seguridad de un formato a otro, simplificando el proceso de intercambio de identidades de usuarios entre dominios de seguridad diferentes.

- **SecureLogin**

SecureLogin [11], es una solución de autenticación basada en directorios que extiende el acceso de inicio único de sesión a prácticamente todas las aplicaciones en el entorno de red multiplataforma. Simplifica la autenticación del usuario a las aplicaciones empresariales proporcionando la experiencia de único logueo, protege contra el acceso no autorizado a las aplicaciones y se integra prácticamente a cualquier dispositivo de autenticación.

- **Enterprise Single Sign On**

Enterprise Single Sign On (Quest) [12], es una solución single sign on basada en las aplicaciones y los inicios de sesión de los usuarios en el sistema sobre identidades existentes en el directorio activo. No requiere una infraestructura difícil de manejar y simplifica tanto la gestión del usuario final y la administración de toda la empresa.

- **TrustBroker Security Solution**

TrustBroker Security Solution [13], solución para aplicaciones SAP, permite comunicaciones seguras dentro de la red corporativa, así como a los proveedores y clientes fuera de la red. Aprovecha las relaciones de confianza individual y a los intermediarios de confianza en las redes cliente/servidor de toda la empresa, ayudando a satisfacer tanto la seguridad de la empresa como los objetivos del negocio.

- **Passlogix**

Passlogix [14], Adquirida por Oracle, permite el Single Sign On integral a través de infraestructura de clave pública, servicios de directorio y de forma independiente. Trabaja prácticamente con cualquier aplicación de Windows, web, propietaria, o basada en host. No requiere integración o scripting. Funciona con Windows Enterprise y aplicaciones cliente-servidor; Mainframe, Unix, AS/400 y otras aplicaciones basadas en host; Microsoft Windows 95, Windows 98, Windows NT, Windows 2000; Microsoft Networking, Novell Netware, Novell NDS client; Entrust/PKI 4.0 and 5.0.

Capítulo 3

Desarrollo del proyecto

En el presente capítulo se expone el proceso de desarrollo del proyecto y se documenta el mismo. Se presentan las tecnologías usadas para llevar a cabo la solución del problema.

El desarrollo realizado en el presente trabajo de grado se llevó a cabo siguiendo las directrices de la metodología de desarrollo ágil *XP (eXtreme programming)*. Se elige la metodología de desarrollo XP, ya que es una metodología ágil que busca que un proyecto avance de manera rápida viendo resultados pronto, haciendo el desarrollo más sencillo aplicando el sentido común, de manera que los artefactos o productos que exige son pocos y se pueden integrar algunos de otras metodologías ajustándose a cada proyecto.

También se tuvo en cuenta el tiempo que se disponía y el entorno para llevar a cabo este trabajo de grado, teniendo en cuenta que se iba a realizar en modalidad pasantía por lo cual se debía entregar a tiempo y con los objetivos cumplidos, por lo tanto se tomaron en cuenta factores como la curva de aprendizaje que se debía tener en cuanto al tema, conocer la infraestructura de la empresa, el equipo de trabajo.

Por lo tanto el desarrollo se llevó a cabo implementando dos herramientas, analizándolas y poniéndolas en marcha para posteriormente hacer las respectivas pruebas y comparar resultados. La primera herramienta es software libre llamada *Metapass SSO* y la segunda herramienta software licenciado llamada *Enterprise Single Single On Manager E-SSOM*. En los puntos 3.2 y 3.3 se muestran el diseño y la implementación respectiva de las herramientas.

3.1 Análisis

XP define como regla fundamental la planeación constante, y para esto tiene como artefacto la redacción de historias de usuario. Se elaboraron las historias principales que describen las funcionalidades principales que se requieren que tenga la aplicación.

3.1.1 Especificación de requerimientos

Para apoyar las historias de usuario y al proceso en general se definió la especificación de requerimientos para determinar el alcance que debía tener la aplicación.

En la tabla 3.1 se muestran los requerimientos funcionales del módulo de usuarios.

	Especificación de Requerimientos ISO-9000 Universidad del Valle	Documento: ER-001	Revisión: 001
Sistema centralizado de autenticación y autorización “Single Sign On”			Fecha:

1. Modulo Usuarios	
Req.	Descripción
R 1.1	El sistema en el módulo usuarios, deberá permitir la validación de usuarios con el directorio activo de la empresa (Windows server 2008)
R 1.2	El sistema deberá permitir que los usuarios puedan acceder a las aplicaciones de acuerdo a los permisos que tengan.
R 1.3	Los usuarios deben autenticarse una vez a cada aplicación a la que tengan permisos.
R 1.4	Si el usuario ingresa la contraseña errónea a la aplicación, el sistema debe volver a pedirle la contraseña.
R 1.5	Al usuario autenticarse a las aplicaciones, las credenciales deben ser encriptadas bajo algún algoritmo para aumentar la seguridad

Tabla 3.1: Requerimientos funcionales, módulo de usuarios.

El documento completo de especificación de requerimientos está contenido en el anexo A.

3.1.2 Historias de usuario

Analizando el problema y las funcionalidades necesarias determinadas se produjeron las historias de usuario generales.

En la tabla 3.2 se muestran las historias de usuario definidas.

	Definición Historias de usuario	Documento: HU-001
Sistema centralizado de autenticación y autorización “Single Sign On”		Fecha:
Título	Descripción	
COMO usuario QUIERO conectarme a mis aplicaciones logueándome solo una vez a cada una de ellas PARA acceder luego rápidamente	Al abrir por primera vez la aplicación, el usuario se podrá loguear, entrando a la aplicación y dejando sus credenciales guardadas.	
COMO usuario QUIERO que el proceso de cambiar contraseñas sea transparente PARA no tener que memorizar nuevas contraseñas	Cuando alguna aplicación requiera cambio de contraseña, el sistema la cambiará escogiendo una contraseña aleatoria con parámetros establecidos, haciendo este proceso transparente al usuario.	
COMO usuario QUIERO ingresar a mis aplicaciones desde el navegador Chrome PARA más tener una mejor experiencia en mis aplicaciones	Las aplicaciones se pueden usar en el navegador Internet Explorer y en Google Chrome ya que trae su plugin respectivo para hacer esto posible.	
COMO usuario QUIERO ingresar desde mi dispositivo móvil	En una versión posterior a la adquirida esta característica estará disponible para todos los usuarios.	

PARA poder conectarme aun estando fuera de la oficina	
---	--

Tabla 3.2: Historias de usuario

3.2 Diseño

3.2.1 Arquitectura

3.2.1.1 Metapass SSO

Metapass SSO⁹ tiene tres componentes principales y permite a los usuarios acceder a múltiples sistemas de seguridad con una solo autenticación sin la necesidad de escribir y recordar múltiples contraseñas.

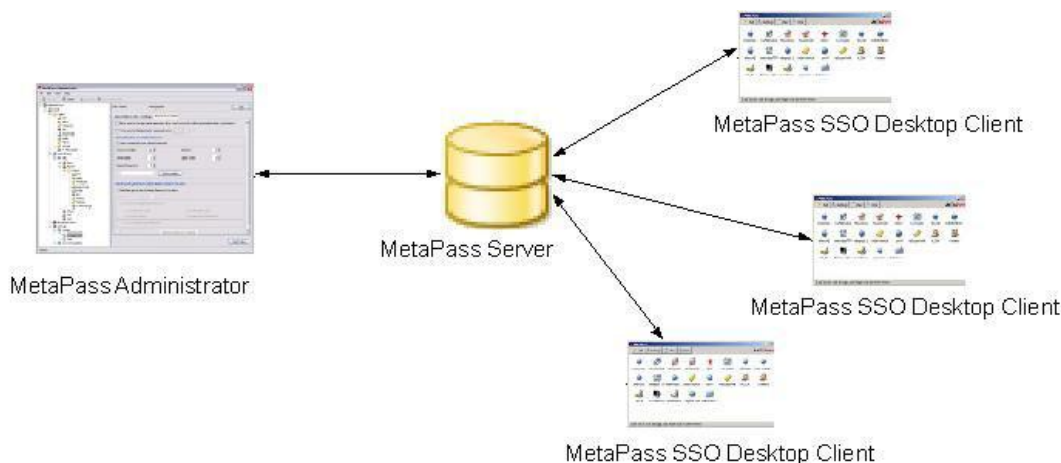


Figura 3.2: Arquitectura Metapass SSO

MetaPass Server: MetaPass utiliza la arquitectura cliente- servidor para gestionar cada cliente Desktop SSO. El servidor MetaPass almacena todos los datos y archivos de configuración del Administrador MetaPass. También distribuye las actualizaciones a los clientes Desktop SSO y gestiona copias de seguridad de los clientes.

MetaPass Administrator: MetaPass Administrator es una aplicación cliente de administración para el personal de TI. Creación de nuevos perfiles de aplicación, la creación de esquemas de autenticación, incluir usuarios y aplicar políticas a los clientes se llevan a cabo en esta herramienta. Todos los datos de esta herramienta se almacenarán en el servidor.

⁹ Metapass SSO guide, disponible en: <http://sourceforge.net/projects/metapass/files/>

MetaPass SSO Desktop: SSO Desktop es una aplicación cliente para los usuarios finales. En realidad ejecuta el proceso de inicio de sesión único para los usuarios. Recibe actualizaciones de perfiles de aplicaciones y actualizaciones de políticas desde el servidor cada que estén disponibles.

3.2.1.2 E-SSOM (*Enterprise single sign manager*)

E-SSOM se basa en la arquitectura cliente-servidor el cual es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores y los demandantes, llamados clientes. También conocida como arquitectura de tres capas.

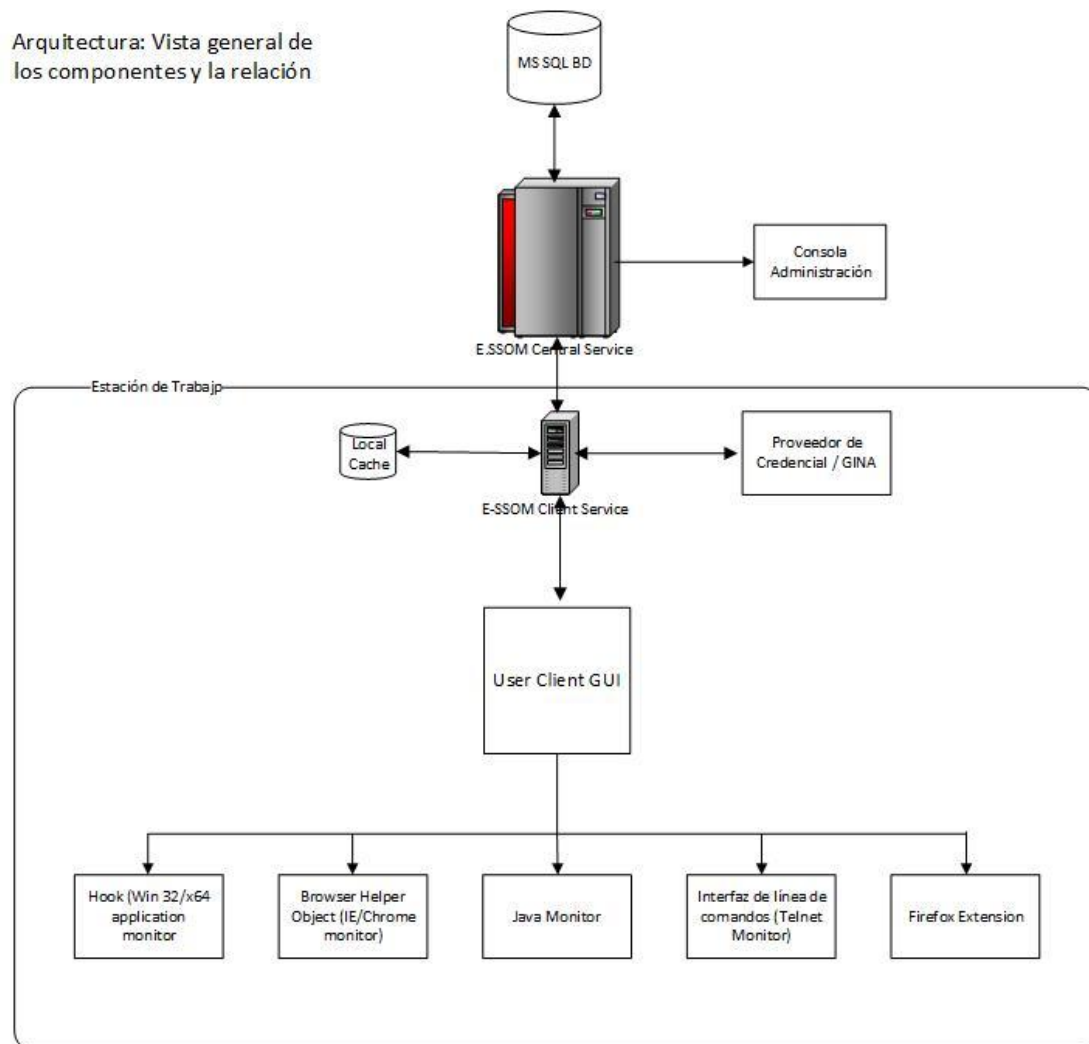


Figura 3.3: Arquitectura E-SSOM¹⁰

E-SSOM¹⁰ está compuesto por muchos componentes que se comunican uno con el otro. Algunos de estos componentes también almacenan (encriptada) la información en una base de datos o en archivos.

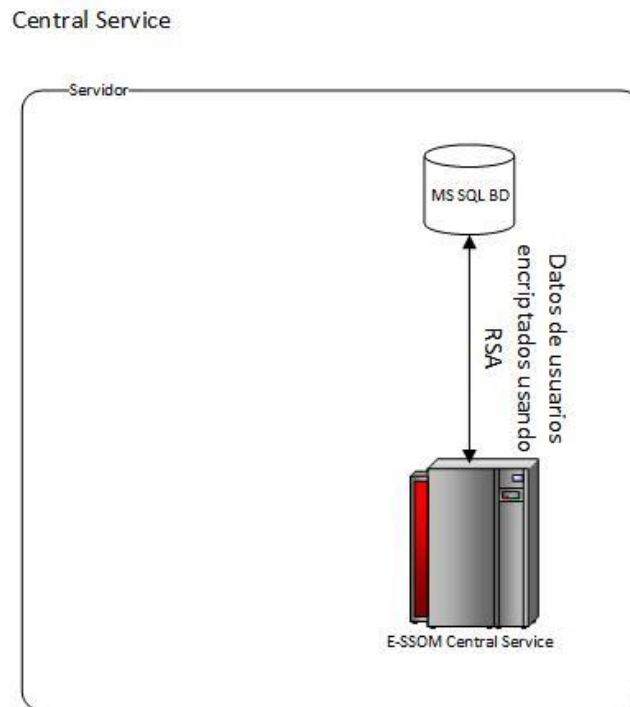


Figura 3.4: Central Service¹⁰

El principal componente de E-SSOM es el *central service* o servicio central. Este servicio administra todas las conexiones con los clientes, así como la conexión con la base de datos E-SSOM. El *central service* de E-SSOM puede ser instalado en cualquier servidor en la red. La base de datos MSSQL no es necesario que esté instalada en la misma máquina.

Seguridad: Todos los datos de usuario que son almacenados en la base de datos E-SSOM se cifran usando RSA con una longitud de clave de 1024 bits.

Redundancia

E-SSOM está diseñado de manera que pueda ser configurado para situaciones de alta disponibilidad. Hay varios mecanismos que se pueden usar para lograr una alta disponibilidad como:

Modo sin conexión del usuario cliente: El cliente usuario puede ser configurado de manera que la caché del usuario y los datos de configuración estén de forma local en el equipo cliente. Esto permite a los usuarios seguir trabajando con E-SSOM aunque el servicio central no está disponible. La funcionalidad proporcionada por el modo sin conexión del usuario cliente también se puede utilizar en los portátiles que no siempre están conectados a la red de la empresa. Cuando los portátiles se conectan a la red, se comunican con el servicio central

¹⁰ E-SSOM Architecture.pdf

para el intercambio de datos. Estos datos son almacenados localmente de modo que el usuario puede seguir usando E-SSOM cuando trabaja en casa o en otro lugar.

Múltiples Servidores Centrales E-SSOM: Más de un servidor central pueden ser instalados para proporcionar una alta disponibilidad en caso de alguna falla de *hardware* en uno de los servidores que ejecuta el servicio central E-SSOM. Los clientes se conectarán automáticamente a otro servidor si la conexión con el servicio central falla.

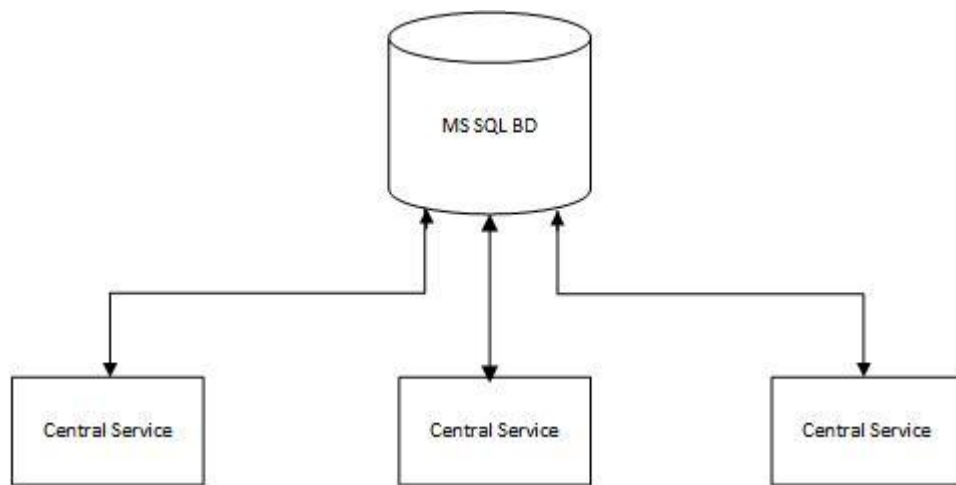


Figura 3.5: Múltiples servicios centrales¹⁰

Múltiples bases de datos E-SSOM: En combinación con los múltiples servidores centrales E-SSOM, múltiples bases de datos E-SSOM deben ser usadas. Las bases de datos deben ejecutarse en un servidor MSSQL y replicar los datos almacenados en la base de datos a las otras bases de datos E-SSOM.

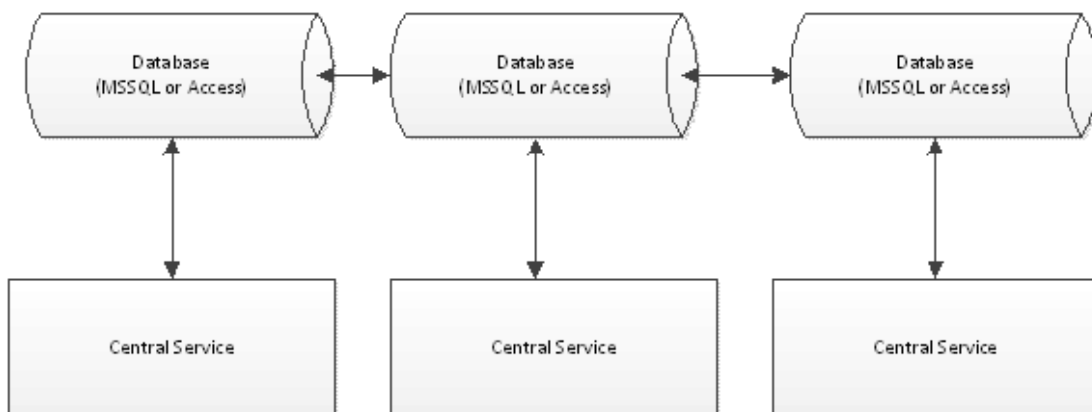


Figura 3.6: Múltiples bases de datos¹⁰

Client Service

El E-SSOM *client service* está instalado en las estaciones de trabajo. Este servicio mantiene la conexión entre el cliente y el *central service*, realiza un seguimiento de las sesiones del cliente y gestiona la memoria caché local. El E-SSOM *client service* es el único componente de la máquina cliente que almacena información.

Caché local: La caché local contiene todos los datos de configuración de E-SSOM. Esto reduce al mínimo la cantidad de datos que deben ser comunicados entre el E-SSOM *Central Service* y el *Client Service*. Si el modo sin conexión está habilitado, la memoria caché local también contiene datos de usuario cifrados. Los datos se encriptan usando Triple DES.

Seguridad: El *Client Service* se comunica con el *Central Service* utilizando un cifrado de 128 bits RC4 conexión RPC. Si el *Client Service* está configurado como un cliente de internet, el *Client Service* se comunicará mediante RPC a través de HTTP (usando SSL). La conexión RPC cifrada se hace a través de un túnel con una conexión https.

El *Client Service* se comunica con sus componentes locales mediante conexiones cifradas LPC.

User Client GUI

El E-SSOM *User Client GUI* está instalado en las estaciones de trabajo. No sólo proporciona una interfaz de usuario que permite a los usuarios llevar a cabo varias acciones, sino que también controla los diversos componentes que monitorean los eventos de inicio de sesión en las aplicaciones. Si el *User Client* no se está ejecutando, E-SSOM no controlará ningún proceso.

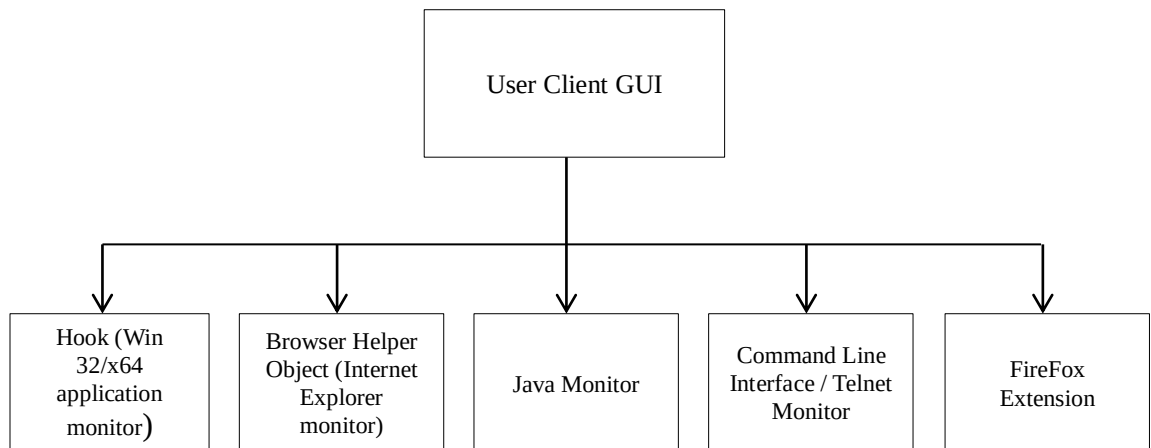


Figura 3.7: User Client GUI¹⁰

Seguridad: El *User Client* se comunica con el *Client Service* utilizando un cifrado de 128 bits RC4 conexión LPC. Los distintos componentes no se comunican con el *User Client* excepto para información de control. Los diversos componentes del monitor se comunican con el *Client Service* mediante una conexión cifrada LPC.

Componentes de Monitoreo

El *software* E-SSOM *User Client* instala varios componentes que monitorean aplicaciones y sitios web para los eventos configurados. Estos componentes son controlados por *User Client*, pero obtienen su configuración y los datos de usuario directamente desde el *Client Service* utilizando una conexión encriptada LPC.

Hook

El E-SSOM *Hook* es un DLL que se usa para controlar las aplicaciones de 32 y 64 bits. También puede monitorear los formularios HTML que están embebidos en aplicaciones. Para evitar conflictos con otros componentes de E-SSOM, varias aplicaciones no son monitoreadas por el *Hook*. Estas aplicaciones son controladas por otros componentes. Las siguientes aplicaciones están excluidas: Internet Explorer, FireFox y la máquina virtual de Java.

Browser Helper Object (BHO)

El E-SSOM *BHO* es un objeto de ayuda del navegador que se utiliza para supervisar los sitios web. El *BHO* puede monitorear los sitios web en Internet Explorer 6 o superior. Los cuadros de diálogo de inicio de sesión en *Internet Explorer* que no son parte de un sitio web también pueden ser controlados por este componente.

Command Line Interface / Telnet monitor

La interfaz de línea de comandos (*CLI*) / Telnet monitor se utiliza para aplicaciones de 'consola'. El '*Command Prompt*' de Windows es tal aplicación.

Java Monitor

El monitor de Java se utiliza para controlar las aplicaciones Java, así como los *applets* de Java en los navegadores. El *Java Monitor* soporta las aplicaciones escritas para Java 1.5 o superior.

FireFox Extension

La extensión de Firefox es una extensión que se utiliza para supervisar los sitios web en Firefox. Los cuadros de diálogo de inicio de sesión en *Firefox* que no son parte de un sitio web también pueden ser controlados por este componente.

3.2.2 Directorio Activo

Para la implementación de las dos herramientas se utilizó el directorio activo o AD (active directory) de la empresa para conectándolo a cada una de las aplicaciones, el directorio activo es Windows Server 2008.

El directorio activo¹¹ es la pieza fundamental del control de la seguridad de IT e identidad en las organizaciones, almacena información sobre objetos en la red, implementa los servicios que permiten que dicha información esté disponible y pueda ser utilizada por los usuarios, máquinas y aplicaciones. El DNS como sistema de nombres jerárquico (integrado con el AD)

¹¹ Capacitación conceptos básicos infraestructura.ppt

y las relaciones de confianza dan una estructura lógica y consistente que organiza los dominios y sus recursos de forma predecible y útil.

El directorio activo actúa como intermediario entre cualquier petición de usuario, máquina, aplicación o servicio para permitirles o no el acceso a los recursos de la red, incluidos sistemas de archivos NTFS, aplicaciones web, el kernel, entre otros.

Los *Servicios de Dominio de Active Directory* (AD DS) proporcionan la funcionalidad de una solución de identidad y acceso (IDA) para redes de empresas. La solución IDA es necesaria para mantener la seguridad de los recursos de la empresa tales como archivos, correo electrónico, aplicaciones y bases de datos.

Una infraestructura IDA debería realizar lo siguiente:

Almacenar información sobre usuarios, grupos, ordenadores y otras identidades, autenticar una identidad, control de acceso y auditoría.

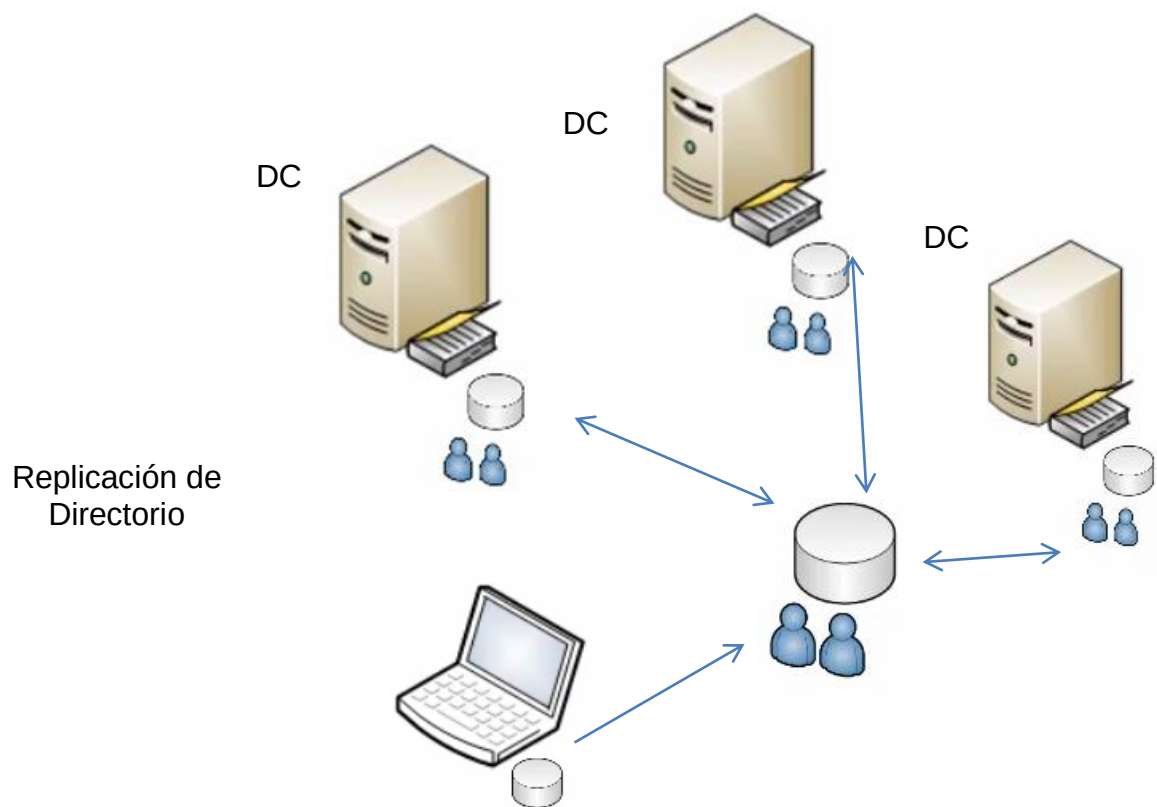


Figura 3.8: Replicación de Directorio¹¹

Dominio

La menor unidad constructiva para poder utilizar Active Directory es el dominio y se define como un conjunto arbitrario de recursos de red bajo una administración común, tal que se cumpla: Límite de administración (los administradores sólo tendrán poder de administración sobre el), límite de seguridad (los administradores definirán los requerimientos de seguridad en sus dominios), límite de replicación (la información sensible de los recursos de red no se replicará fuera de sus límites).

Controlador de Dominio (DC)

Cuando se promueve un servidor de Directorio Activo a un Dominio este se transforma en un DC. Las funciones fundamentales de los Controladores de Dominio son proveer la validación de los usuarios y equipos; y la replicación de la información del directorio a otros Controladores de Dominio del mismo dominio.

Estructura Lógica

Se pueden instalar varios dominios, éstos se pueden agrupar en estructuras jerárquicas denominadas árboles (*Trees*).

Para poder construir un árbol (*Tree*) se debe comenzar por crear el primer dominio en la estructura, a partir del cual se crean los subdominios.

Unidad Organizativa

Es un contenedor que se utiliza para organizar objetos dentro de un dominio que facilita la manejabilidad y visibilidad.

Usuarios

Es un objeto que almacena la información referente a los usuarios que se autentican en el Directorio Activo.

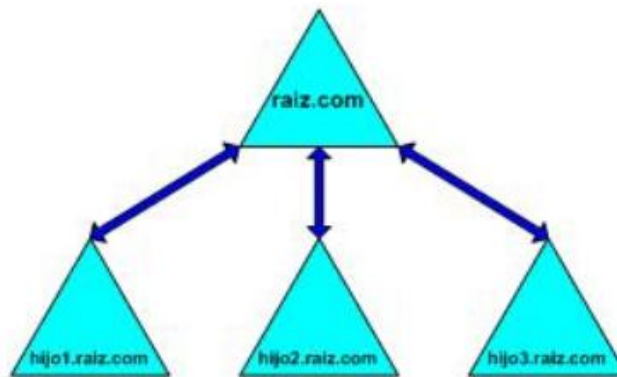


Figura 3.9: Estructura lógica del AD¹¹

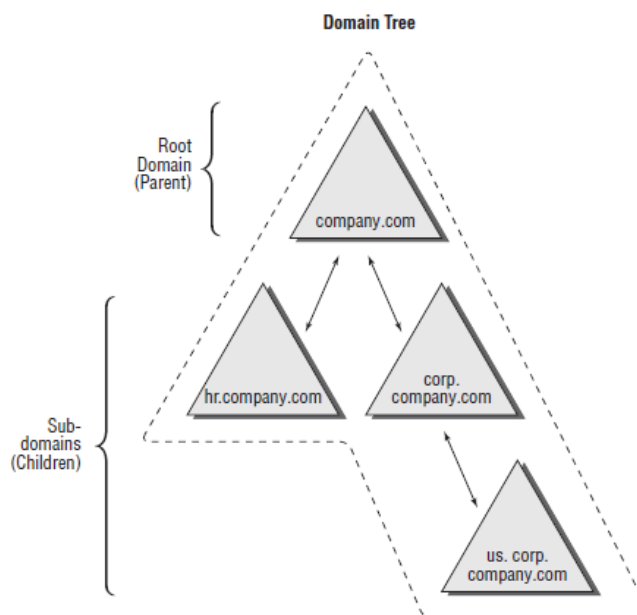


Figura 3.10: Árbol de dominio¹¹

Windows Server 2008 ofrece soluciones específicas bajo los distintos roles asociados al AD como servidor de dominio, servicios de LDAP, servicios de certificados o servicios de gestión de derechos.

Servicios de Dominio (AD DS)¹²

Active Directory Domain Services (AD DS) mantiene la información de los usuarios, máquinas y dispositivos de la red y permite gestionar de forma segura esta información y facilitar la colaboración e el uso compartido de los recursos entre usuarios. AD DS se necesita también para ciertas aplicaciones como Microsoft® Exchange Server y para tecnologías de gestión centralizada, como las Políticas de Grupo.

Servicios de Certificados (AD CS)¹²

Active Directory® Certificate Services (AD CS) es un servicio parametrizable para la creación y administración de certificados de clave pública, necesarios para el empleo de tecnologías de infraestructura de clave pública (PKI).

Servicios de Gestión de Derechos (AD RMS)¹²

AD RMS es una tecnología de protección de la información que funciona con aplicaciones compatibles para impedir el uso no autorizado de información digital. Los propietarios de los contenidos pueden determinar exactamente el modo de uso de la información: quien puede abrirla, modificarla, imprimirla, reenviarla, etc. e incluso crear plantillas de aplicación de derechos como por ejemplo "Confidencial - Sólo lectura" que persisten a través de todo el ciclo de vida de los documentos. Estas políticas se aplican incluso cuando los documentos abandonan la red corporativa.

¹² <http://technet.microsoft.com/en-us/windowsserver/bb310558.aspx>

Servicios de Federación de Identidades (AD FS)¹²

Active Directory Federation Services (AD FS) habilita las tecnologías de logon único (SSO) para Web que permiten autenticar a un usuario a través de múltiples aplicaciones Web empleando la misma cuenta de usuario para todas ellas. AD FS lo hace posible mediante la federación (es decir, compartir la información entre diferentes organizaciones independientes entre sí) de las identidades de usuario y derechos de acceso, en forma de peticiones digitales entre organizaciones que establecen entre ellas una relación de intercambio de datos.

Servicios de LDAP para aplicaciones (AD LDS)¹²

El rol de servidor de Active Directory® Lightweight Directory Services (AD LDS) es un servicio de directorio LDAP (Lightweight Directory Access Protocol). Permite realizar operaciones de almacenamiento y recuperación de información de directorio para aplicaciones basadas en directorios sin las restricciones impuestas por el rol de Servicios de Dominio (AD DS).

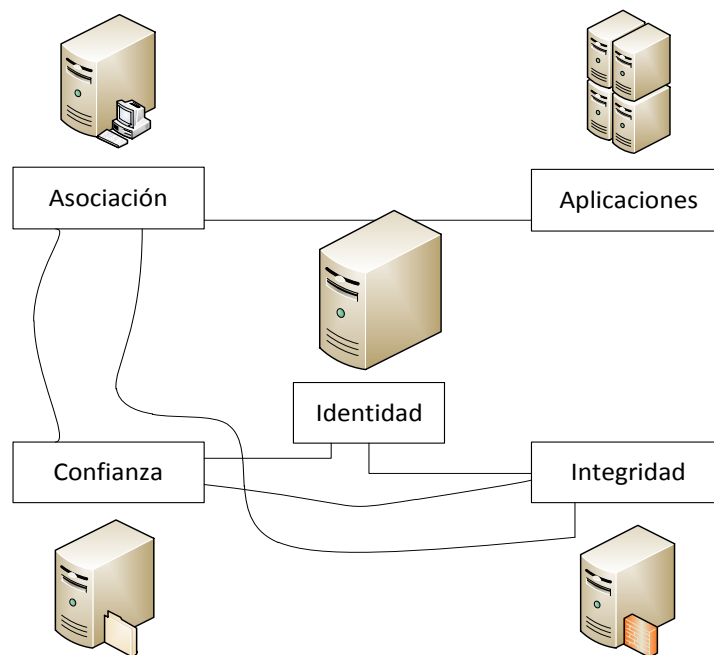


Figura 3.11: Tecnologías de Active Directory

En la estructura es importante mantener los objetos del directorio activo debidamente estandarizados y en la OU (unidad organizativa) donde deben pertenecer.

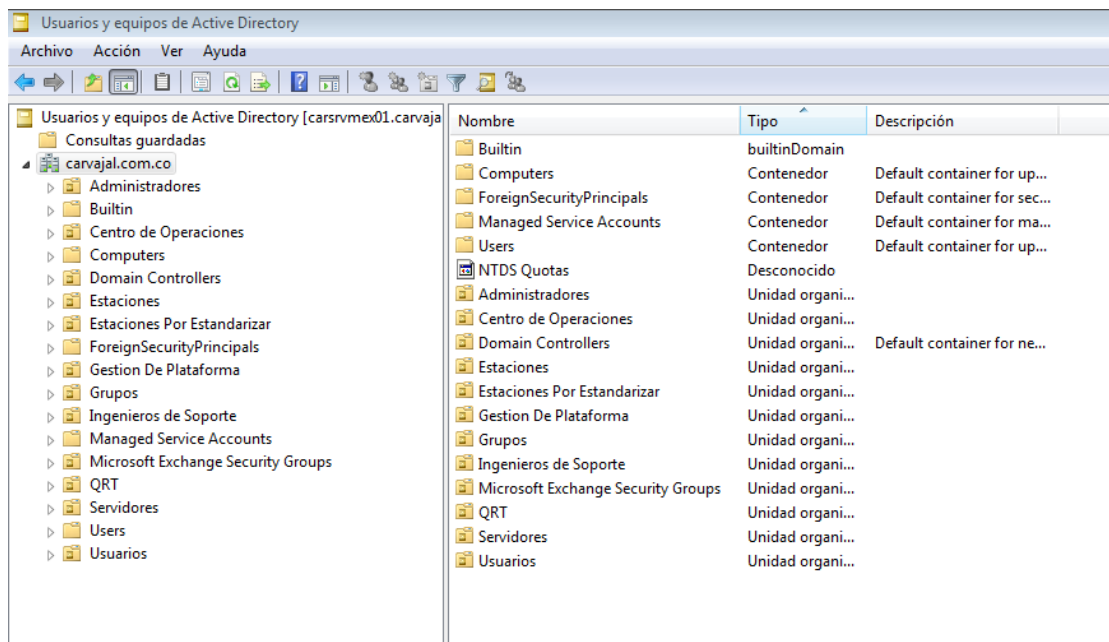


Figura 3.12: Estructura general (OU)

En la unidad organizativa (OU) “Usuarios”, se encuentran organizados los usuarios organizados por empresa y a su vez por área de trabajo, cada una de éstas son las respectivas unidades organizativas.

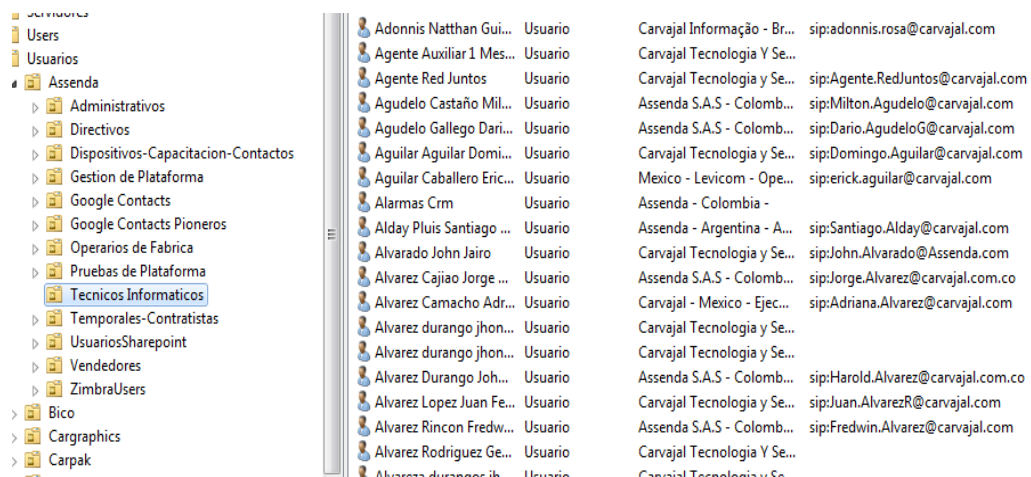


Figura 3.13: OU Usuarios

Cada usuario tiene sus respectivas propiedades, como datos de usuario, área de trabajo, correo electrónico, grupos de los cuales es miembro, entre otras.

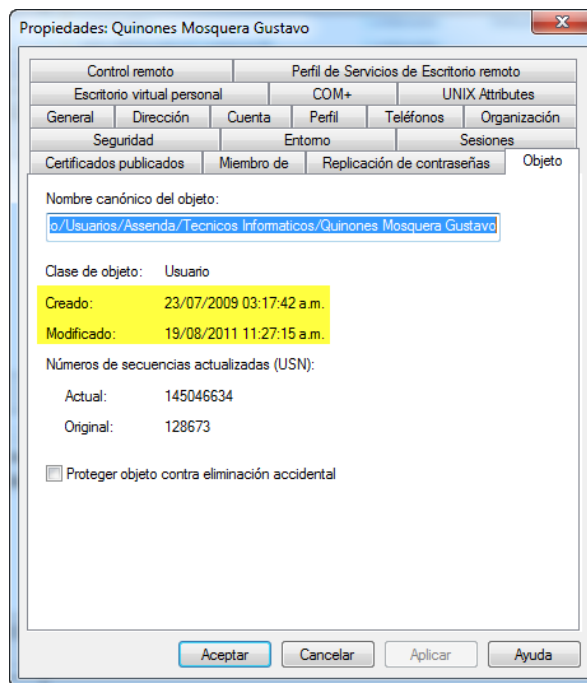


Figura 3.14: Propiedades usuarios

Grupos

Se utilizan para coleccionar usuarios, equipos y otros grupos para crear un único punto de administración.

Equipos

Se representa como una cuenta y objeto en el directorio activo, de hecho inicia sesión en el dominio tal y como lo haría un usuario.

GPO (Group Policy Object)

Es una característica de Windows que permite administrar los cambios de usuarios y equipos desde un punto central de administración. En un entorno administrado por GPO poca o ninguna configuración se debe realizar directamente por contacto en un equipo de escritorio, todas las configuraciones se definen, se refuerzan y se actualizan por medio de las GPO.

Autenticación

La autenticación es el proceso con el que se demuestra ser alguien que se dice. Eso es, se dice ser determinado usuario y se demuestra introduciendo la contraseña del mismo. El sistema verifica que la contraseña sea la correcta, lo cual prueba que es quien dice ser determinado usuario.

Autorización

La autorización es verificar que el usuario tenga los privilegios necesarios para acceder al recurso y en la forma solicitada.

3.2.3 Base de Datos

3.2.3.1 Metapass SSO

Cuando se utiliza por primera vez, se debe definir la Autenticación y Almacenamiento para el cliente Desktop SSO. Los dispositivos de almacenamiento son usados para almacenar los datos de los usuarios que incluyen las credenciales de cada usuario, definiciones de flujos de trabajo para perfil de aplicaciones y configuración de políticas de usuario. La autenticación se utiliza para proteger todos los datos del usuario que son almacenados en los dispositivos de almacenamiento. MetaPass proporciona una herramienta visual altamente configurable llamada *Authentication and Storage Editor*¹³ para configurar los clientes Desktop SSO.

Hay tres configuraciones usadas comúnmente disponibles como plantillas.

Windows Authentication Template



Figura 3.15: Autenticación Windows

Esta es la configuración más común para los usuarios de Windows. Mediante el uso de esta configuración, los usuarios se autentican por Windows o por el dominio, si estos son usuarios de dominio. Las credenciales del usuario están protegidas por *Windows Crypto API (DPAPI)*. En esta configuración cuando el Desktop SSO está guardando los datos del usuario, los datos serán cifrados por *Windows Crypto API* en primer lugar, y luego se guardan en un archivo llamado *creds.xml*. En el proceso de lectura los datos son descifrados por *Windows Crypto API*¹³.

Master Password Template

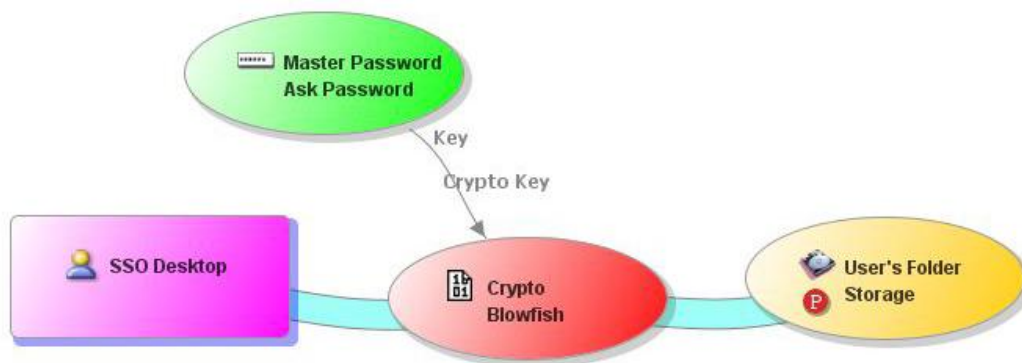


Figura 3.16: Contraseña maestra

¹³ MetaPass_Admin_Auth_Storage_Guide_4_6_rev0109.pdf, disponible en <http://sourceforge.net/projects/metapass/files/>

Esta configuración es común para ambientes que no sean Windows. *Crypto Plug-in* se utiliza para proteger los datos del usuario. Se puede elegir cualquiera de los métodos de cifrado como *Blowfish*, *DES*, *AES* y *3DES*. Sin embargo, estos métodos criptográficos necesitan una clave de cifrado para cifrar y descifrar datos. El Plug-in contraseña maestra se utiliza para proporcionar una clave de estos *Crypto Plug-in*¹³.

KIOSK Template

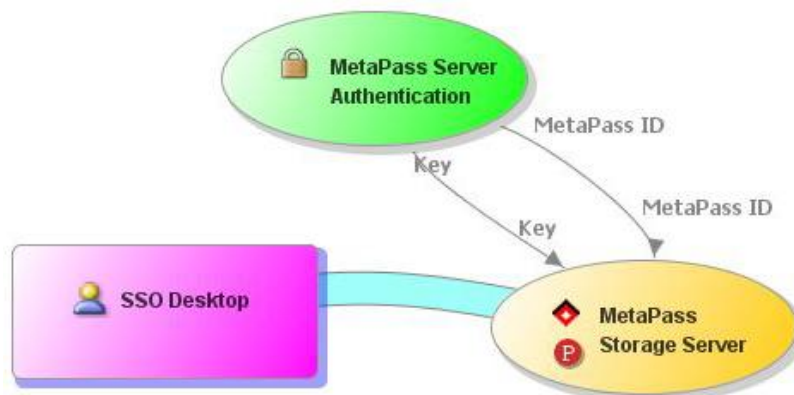


Figura 3.17: KIOSK

El servidor Metapass ofrece dos servicios de esta configuración: Almacenamiento de datos del usuario y la autenticación de usuarios. El servidor tiene embebida una base de datos para almacenar los datos del usuario, y se conecta al servidor de dominio para autenticar. Para los usuarios sin dominio, se genera una contraseña única después de la inscripción de un usuario, y será utilizada para la autenticación con el servidor.

Windows Crypto API

En este caso se escogió como sistema de autenticación Windows Crypto API¹⁴. A partir de Microsoft Windows 2000, el sistema operativo comenzó a proporcionar una interfaz de programación de aplicaciones de protección de datos (API). Esta API de protección de datos (DPAPI) es un par de llamados de funciones que proporcionan los servicios de protección de datos a nivel de sistema operativo a los usuarios y procesos del sistema. En cuanto a protección de datos es un servicio que proporciona confidencialidad de los datos mediante cifrado. DPAPI es un servicio de protección basado en contraseñas, por lo tanto se requiere de una contraseña para proporcionar protección. La desventaja por supuesto, es que toda la información contemplada por DPAPI se basa en la contraseña proporcionada; esto se ve compensado por DPAPI mediante rutinas criptográficas, concretamente el algoritmo Triple-DES y claves fuertes. Debido a que DPAPI se centra en proporcionar protección para los usuarios y requiere una contraseña para proporcionar esta protección, lógicamente, utiliza la contraseña de inicio de sesión del usuario para la protección.

¹⁴ <http://msdn.microsoft.com/en-us/library/ms995355.aspx>

Arquitectura DPAPI¹⁴

Las aplicaciones pasan los datos en texto plano a DPAPI y reciben un BLOB de datos protegidos, o pasan el BLOB de datos protegidos a DPAPI y reciben los datos en texto plano. La siguiente figura muestra estas dos operaciones.

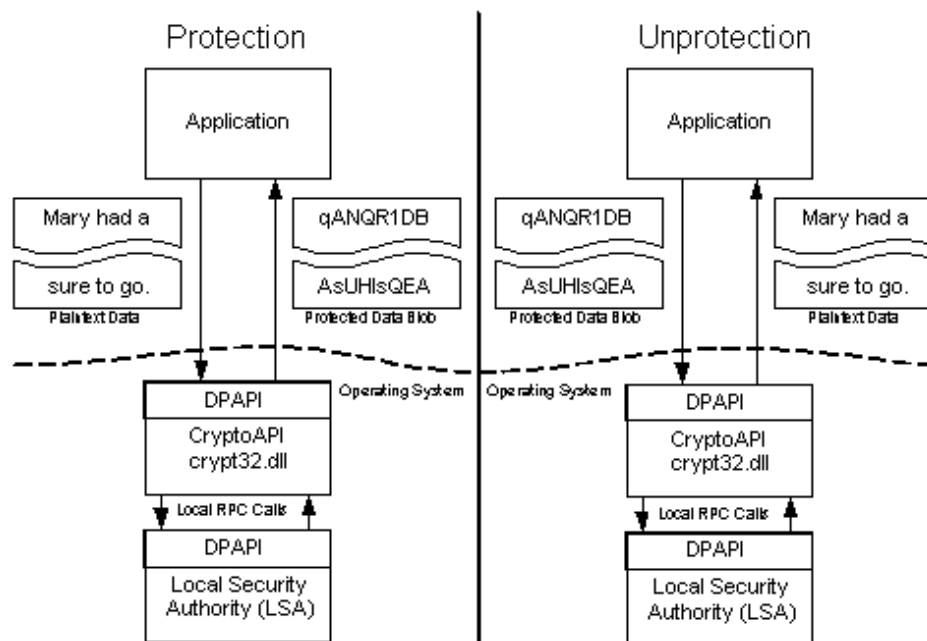


Figura 3.18: DPAPI es una API¹⁴

El BLOB de datos protegido, es una estructura opaca que además de los datos cifrados, también contiene los datos para permitir a DPAPI desprotegerlos. Un punto importante es que DPAPI se limita a aplicar la protección criptográfica a los datos.

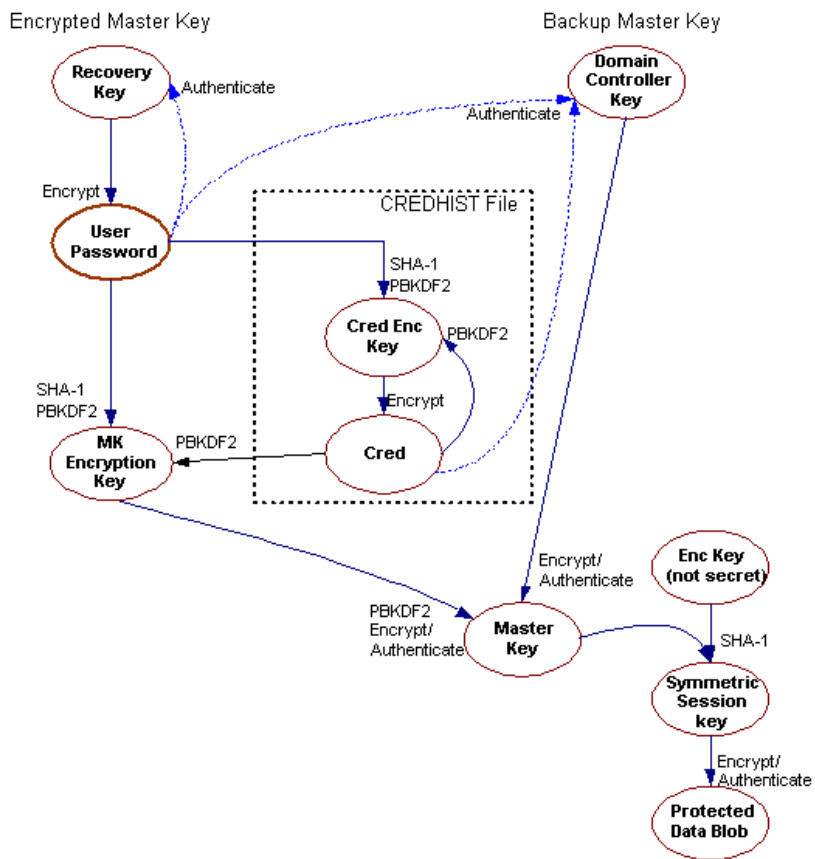
Un pequeño inconveniente de utilizar la contraseña de inicio de sesión es que todas las aplicaciones que se ejecutan en el mismo usuario pueden acceder a los datos protegidos que se conocen. Por supuesto, ya que las aplicaciones deben almacenar sus propios datos protegidos, el acceso a los datos podría ser algo difícil para otras aplicaciones, pero ciertamente no es imposible.

Para contrarrestar esto, DPAPI permite que una aplicación utilice un secreto adicional para la protección de datos. Este secreto adicional es requerido entonces para desproteger los datos. Técnicamente, este "secreto" debe ser llamado entropía secundaria.

Es secundario porque, si bien no refuerza la clave utilizada para cifrar los datos, aumenta la dificultad de una aplicación que se ejecuta bajo el mismo usuario, cuando se compromete la clave de cifrado de otra aplicación.

La entropía que significa transformación, mide tanto la falta de información como la información y puede ser usada como una medida para reducir o eliminar la incertidumbre, en este caso analiza el grado de homogeneidad (ya que se está analizando un mismo usuario) y así bien ésta entropía secundaria es utilizada para descifrar los datos.

Relación de claves

Figura 3.19: Relación de claves¹⁴

El círculo en negrilla indica el centro de las relaciones de clave DPAPI: la contraseña de usuario. En los sistemas autónomos, la clave de recuperación protege la contraseña para permitir a los usuarios restablecer sus contraseñas con el PRD. La contraseña de usuario se utiliza para derivar la clave de cifrado de llave maestra, la cual se utiliza para proteger la llave maestra. Por último, una derivación de la contraseña, la credencial de usuario, se almacena en el archivo "Historia de credenciales", que permite a DPAPI acceder a MasterKeys protegidos por contraseñas antiguas.

En estaciones de trabajo, un controlador de dominio de clave pública, también protege la llave maestra. Esto permite a DPAPI acceder a un controlador de dominio y restaurar la llave maestra, si no se puede utilizar la clave de cifrado de llave maestra. Por último, la llave maestra se utiliza para derivar la clave de sesión simétrica, que protege los datos de la aplicación.

3.2.3.2 E-SSOM

Para utilizar el software E-SSOM se debe tener un sistema gestor de base de datos instalado, en este caso Microsoft SQL server 2008¹⁵. Sus lenguajes para consultas son T-SQL y ANSI SQL.

Entre sus características se encuentran, soporte de transacciones, soporta procedimientos almacenados, incluye entorno gráfico de administración que permite el uso de comandos DDL y DML gráficamente.

Permite trabajar en modo cliente-servidor, donde la información y datos se alojan en el servidor y los terminales o clientes de la red sólo acceden a la información. Además permite administrar información de otros servidores de datos.

T-SQL

(Transact-SQL) es el principal medio de interacción con el servidor. Permite realizar las operaciones claves en el SQL server, incluyendo la creación y modificación de esquemas de la base de datos, la introducción y edición de los datos en la base de datos, así como la administración del servidor como tal. Esto se realiza mediante el envío de sentencias T-SQL y declaraciones que son procesadas por el servidor y los resultados (o errores) regresan a la aplicación cliente.

Cliente Nativo de SQL

Cliente Nativo de SQL es la biblioteca de acceso a datos para los clientes de Microsoft SQL Server versión 2005 en adelante. Implementa nativamente soporte para las características de SQL Server, incluyendo la ejecución de la secuencia de datos tabular, soporte para bases de datos en espejo de SQL Server, soporte completo para todos los tipos de datos compatibles con SQL Server, conjuntos de operaciones asíncronas, las notificaciones de consulta, soporte para cifrado, así como recibir varios conjuntos de resultados en una sola sesión de base de datos. Cliente Nativo de SQL se utiliza como extensión de SQL Server plug-ins para otras tecnologías de acceso de datos, incluyendo ADO u OLE DB. Cliente Nativo de SQL puede también usarse directamente, pasando por alto las capas de acceso de datos.

Cifrado de datos transparente (TDE)

Se pueden cifrar los datos confidenciales en la base de datos y usar un certificado para proteger las claves que se utilizan para cifrarlos. Esto evita que cualquiera que carezca de las claves utilice los datos.

El cifrado de datos transparente (TDE)¹⁶ realiza el cifrado y descifrado de E/S en tiempo real de los datos y los archivos del registro. El cifrado utiliza una clave de cifrado de la base de datos (DEK), que está almacenada en el registro de arranque de la base de datos para que esté disponible durante la recuperación. La DEK es una clave simétrica protegida utilizando un certificado almacenado en la base de datos maestra del servidor o una clave asimétrica protegida por un módulo EKM. TDE protege los datos “en reposo”, es decir, los archivos de datos y de registro.

¹⁵ http://es.wikipedia.org/wiki/Microsoft_SQL_Server

¹⁶ [http://technet.microsoft.com/es-es/library/bb934049\(v=sql.100\).aspx](http://technet.microsoft.com/es-es/library/bb934049(v=sql.100).aspx)

Arquitectura de cifrado transparente de bases de datos

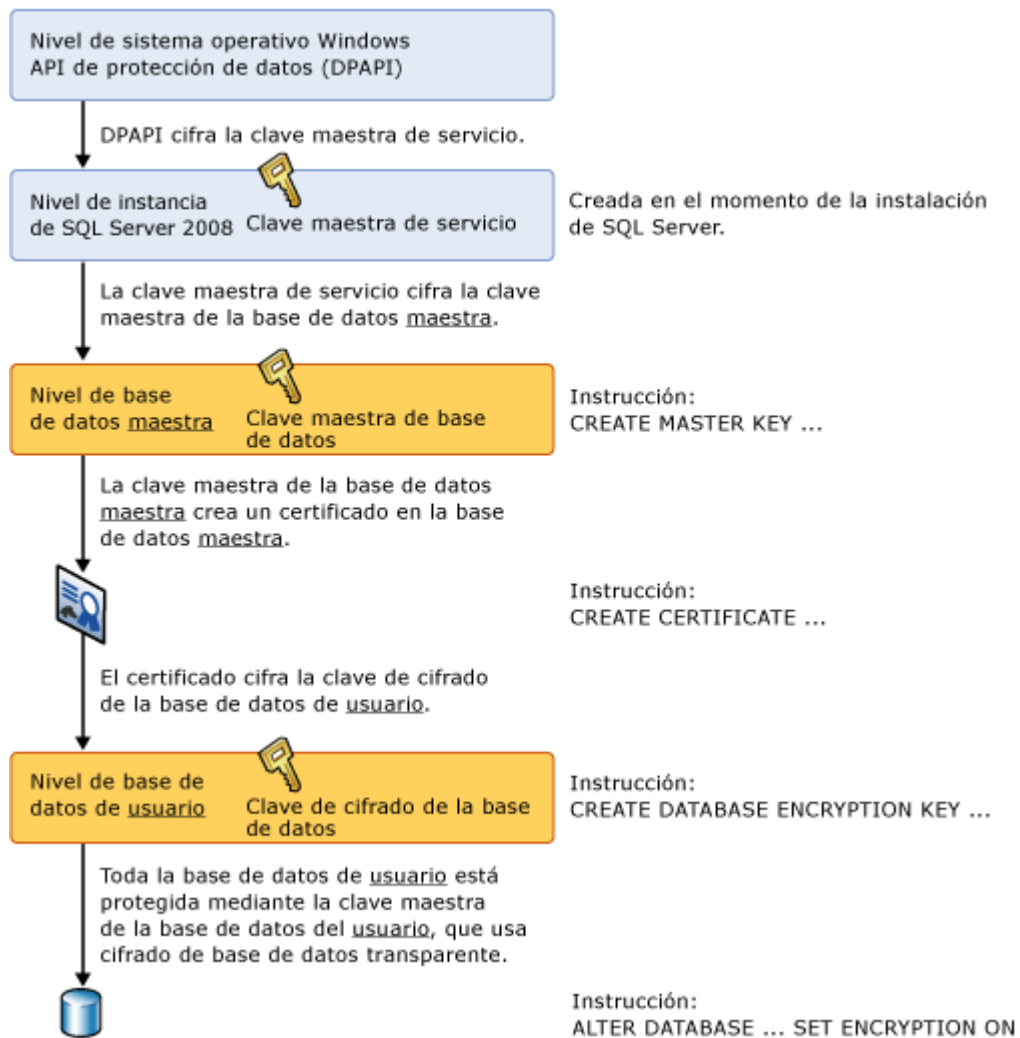


Figura 3.20: Arquitectura del cifrado TDE¹⁶

3.3 Implementación

3.3.1 Metapass SSO

Permite a los usuarios de un computador acceder a múltiples sistemas de seguridad sin tener que recordar e ingresar múltiples contraseñas. Eso también permite a los administradores controlar quien accede a que en la organización, auditar y hacer reportes de eventos. El propósito es incrementar la seguridad y la productividad, garantizar el cumplimiento normativo, mientras se reducen los costos de la mesa de ayuda.

Metapass toma completamente una nueva aproximación para integrar con las aplicaciones. La tecnología de Metapass corre independientemente en Windows, Mac OS, y Linux, en niveles de cliente y servidor. En lugar de ser OSdependiente, opera con

una capa de abstracción más alta que las aplicaciones que se ejecutan, y pone las credenciales directamente en las aplicaciones sin ir a través de las funciones internas del sistema operativo.

Integración universal con todas las aplicaciones

Como resultado, Metapass es totalmente independiente del sistema y trabaja con cualquier aplicación, sin importar como sea la apariencia, como se comporte o que versión sea.

La tecnología de Metapass cae en la virtualización de la interfaz de usuario, haciéndolo completamente independiente de la aplicación y del sistema operativo.

En la primera etapa se instaló, configuró e implementó el software libre Metapass SSO, éste software nos permitió obtener características básicas las cuales se analizaron.

En la configuración se realizó la conexión con el directorio activo, se cargaron los usuarios por unidades organizativas (OU) para que se pudieran conectar respectivamente al programa.

Se configuraron políticas para los distintos grupos, así tenían diferentes privilegios según el área.

Se crearon flujos de trabajo para las distintas aplicaciones, se escogieron algunas para hacer las pruebas, entre ellas Google Apps, SugarCRM, Success Factor, Portal CGA, Portal del colaborador, Portal de la cooperativa, Red Unidos, Skype.

Instalación

Metapass SSO tiene tres componentes principales, los cuales son: Servidor, Consola de administración y Desktop SSO.

Se instaló el servidor de Metapass en una máquina virtual que la empresa dispuso en Bogotá (CTSSSOBOG01) y a la cual se accede remotamente, también se instaló la consola de administración en este mismo servidor. (Ver anexo B: Guía de instalación).

Configuración

El servidor se conectó al directorio activo por conexión LDAP con los siguientes parámetros:

Host: carsrvclo02.carvajal.com.co

Port Number: 389

User DN: CN=Galvez Vidales Laura Estefanía, OU=Tecnicos Informaticos, OU=Assenda,OU=Usuarios,DC=carvajal,DC=com,DC=co

Domain: CARVAJAL.COM.CO

Search Base: OU=Tecnicos Informaticos, OU=Assenda, OU=Usuarios, DC=carvajal, DC=com, DC=co

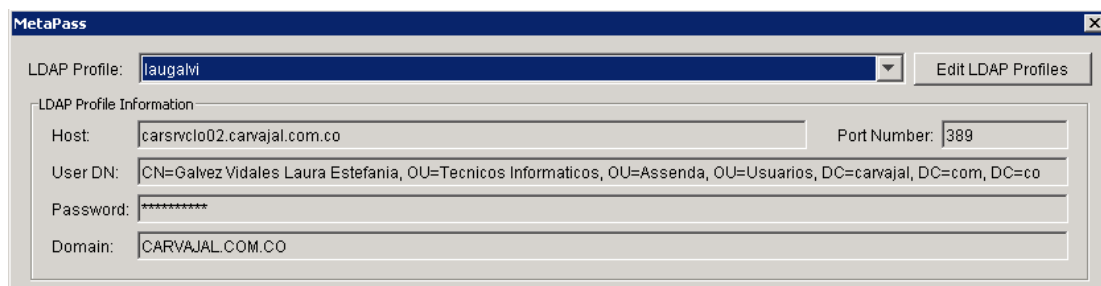
The screenshot shows the MetaPass application window. At the top, there's a title bar 'MetaPass'. Below it, a dropdown menu for 'LDAP Profile' is set to 'laugalvi', with an 'Edit LDAP Profiles' button to its right. A section titled 'LDAP Profile Information' contains several fields: 'Host' is 'carsrvclo02.carvajal.com.co', 'Port Number' is '389', 'User DN' is 'CN=Galvez Vidales Laura Estefania, OU=Tecnicos Informaticos, OU=Assenda, OU=Usuarios, DC=carvajal, DC=com, DC=co', 'Password' is masked with asterisks, and 'Domain' is 'CARVAJAL.COM.CO'.

Figura 3.21: Conexión servidor-directorio activo

Se cargaron los usuarios en la consola de administración por medio de la siguiente conexión:

Administrativos: OU=Administrativos,
OU=Assenda,OU=Usuarios,DC=carvajal,DC=com,DC=co

Técnicos Informáticos: OU=Tecnicos Informaticos, OU=Assenda, OU=Usuarios,
DC=carvajal, DC=com, DC=co

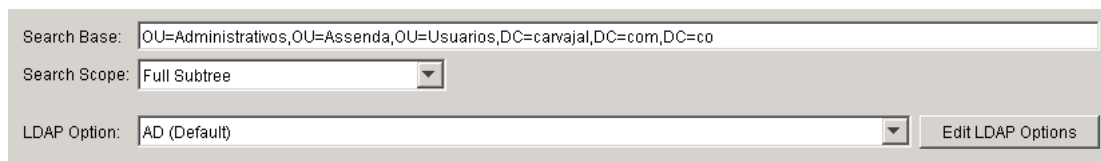
This screenshot shows the LDAP search configuration. The 'Search Base' field contains 'OU=Administrativos,OU=Assenda,OU=Usuarios,DC=carvajal,DC=com,DC=co'. The 'Search Scope' dropdown is set to 'Full Subtree'. The 'LDAP Option' dropdown is set to 'AD (Default)', with an 'Edit LDAP Options' button to its right.

Figura 3.22: Carga de usuarios administrativos

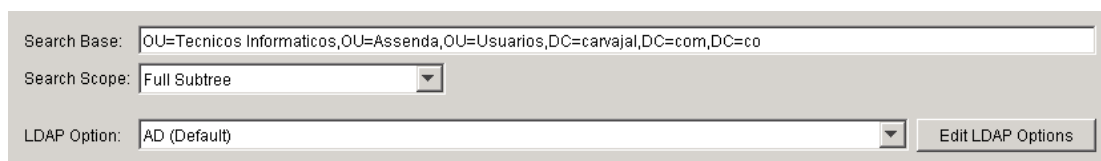
This screenshot shows the LDAP search configuration for technical users. The 'Search Base' field contains 'OU=Tecnicos Informaticos,OU=Assenda,OU=Usuarios,DC=carvajal,DC=com,DC=co'. The 'Search Scope' dropdown is set to 'Full Subtree'. The 'LDAP Option' dropdown is set to 'AD (Default)', with an 'Edit LDAP Options' button to its right.

Figura 3.23: Carga de usuarios Técnicos Informáticos

Creación de flujo de trabajo de las aplicaciones

Para la creación de los flujos de trabajo, se crea el perfil de la aplicación y se crea el proceso de conexión a cada aplicación por medio del editor propio que tiene la aplicación (Metapass SSO editor).

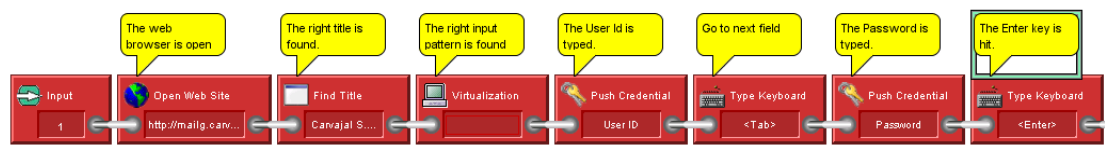


Figura 3.24: Creación flujo de trabajo



Configuración de las aplicaciones a cada usuario

Se configuran las aplicaciones a cada usuario o por grupo.

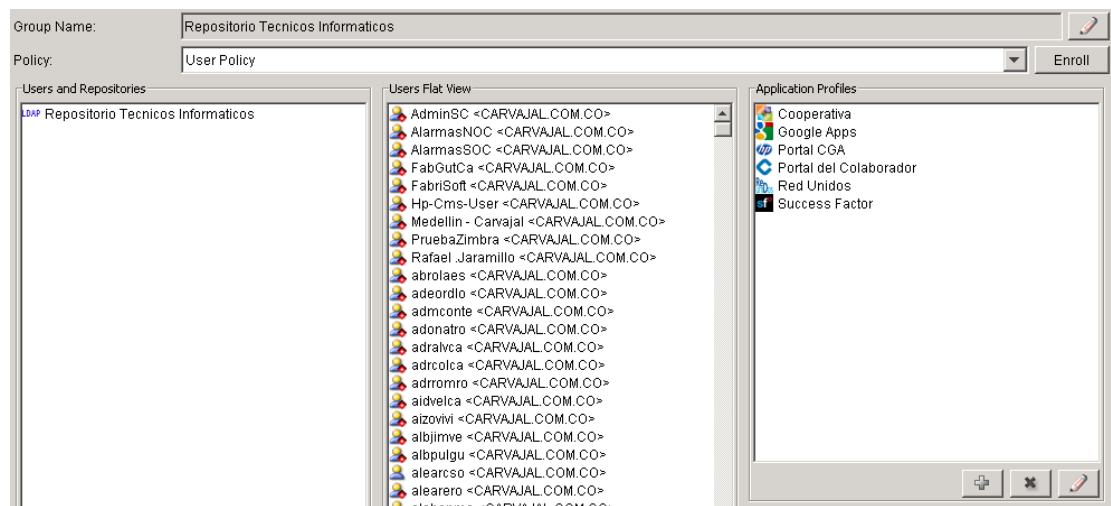


Figura 3.25: Aplicaciones para un grupo (OU)

Instalación del cliente en usuarios finales

Se realizó una fase de pruebas, la cual fue hecha con 100 usuarios a los cuales se les instaló el programa para que lo usaran, lo probaran y posteriormente dieran su opinión acerca de la herramienta.

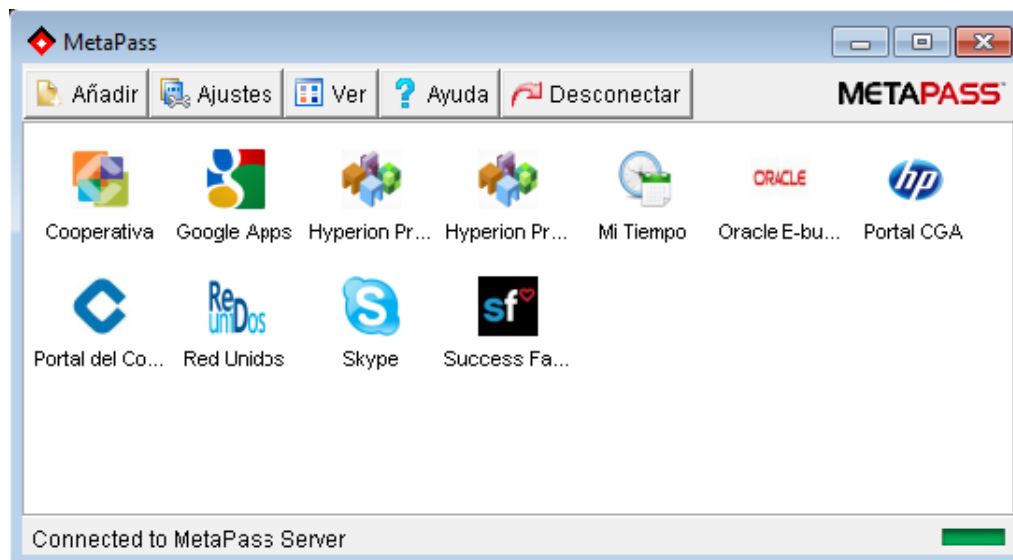


Figura 3.26: Desktop SSO

3.3.2 E-SSOM

Las organizaciones luchan con la gestión de autenticación cada día. E-SSOM permite el fácil uso mediante la utilización de la conexión automática para cada aplicación que se desea utilizar. También cumple con las necesidades al generar un informe sobre las cuentas de usuario que tienen acceso a las aplicaciones, junto con las fechas y las horas de acceso.

También puede proporcionar seguridad adicional con la autenticación de dos factores. Esta autenticación requiere que el usuario final inicie sesión tanto con una tarjeta inteligente y un código PIN. Esto garantiza una autenticación fuerte, ya que se basa en algo que el usuario tiene (la tarjeta inteligente) y algo que sabe (el PIN).

La herramienta E-SSOM es de pago, por lo cual se realizó una reunión virtual con la empresa tools4ever en la cual nos dijeron las características y se negoció un período de prueba para probar la aplicación en la empresa. El piloto consistió en probar con cinco aplicaciones de la empresa, un grupo de usuarios y una licencia por dos meses.

Se realizó la instalación y configuración respectiva, para luego empezar las pruebas con un grupo de usuarios y posteriormente analizar las características y el funcionamiento de la herramienta.

Instalación

E-SSOM consta de un servidor, consola de administración y el cliente. Para iniciar se instaló la base de datos Windows Server 2008 en el servidor CTSSSOBOG01.

Se instaló el servidor E-SSOM y la consola de administración en el mismo servidor, conectando el servidor a la base de datos. (Ver anexo C: Guía de instalación E-SSOM).

Configuración de aplicaciones

En el administrador es donde se crean las aplicaciones que van a ser utilizadas por medio de E-SSOM, se crean los respectivos *scripts* en este caso, algunos son: preguntar_credenciales, guardar_credenciales, click_boton_login, entre otros.

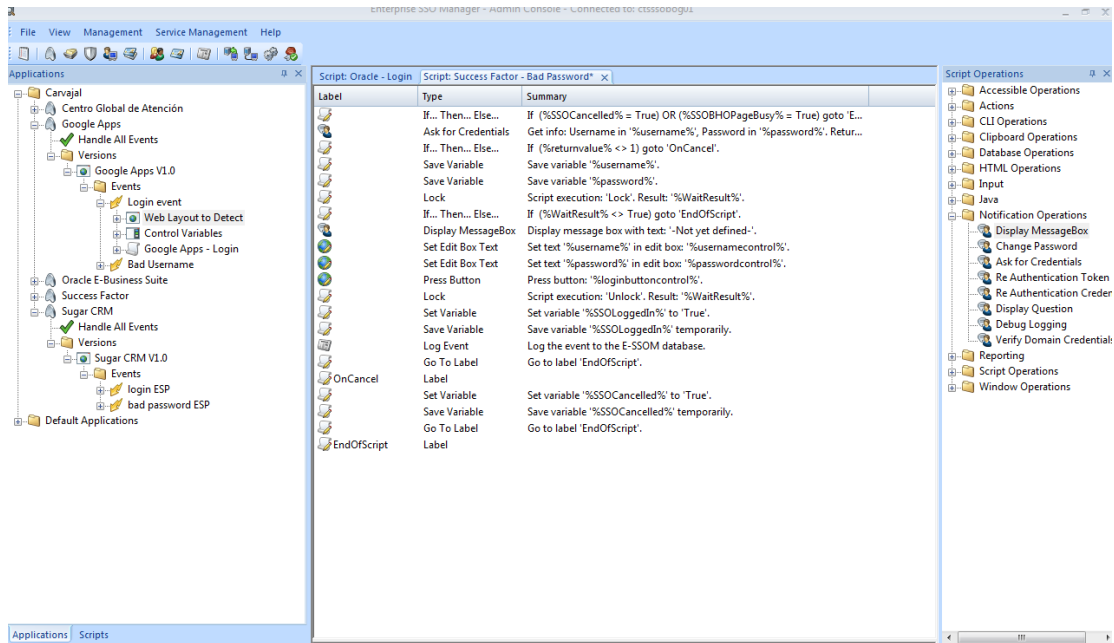


Figura 3.27: Consola de administración

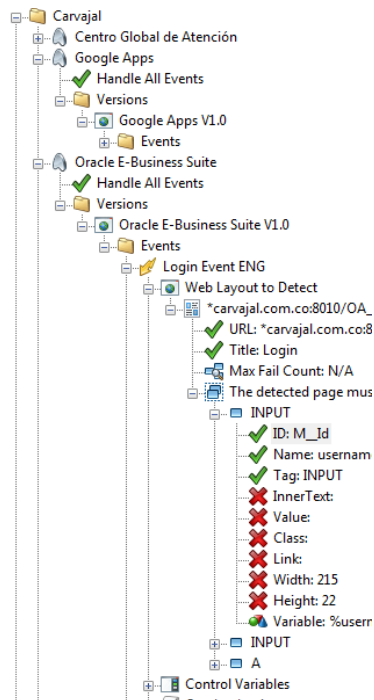


Figura 3.28: Aplicaciones

E-SSOM funciona con la virtualización de interfaz de usuario, así identifica la estructura de las aplicaciones.

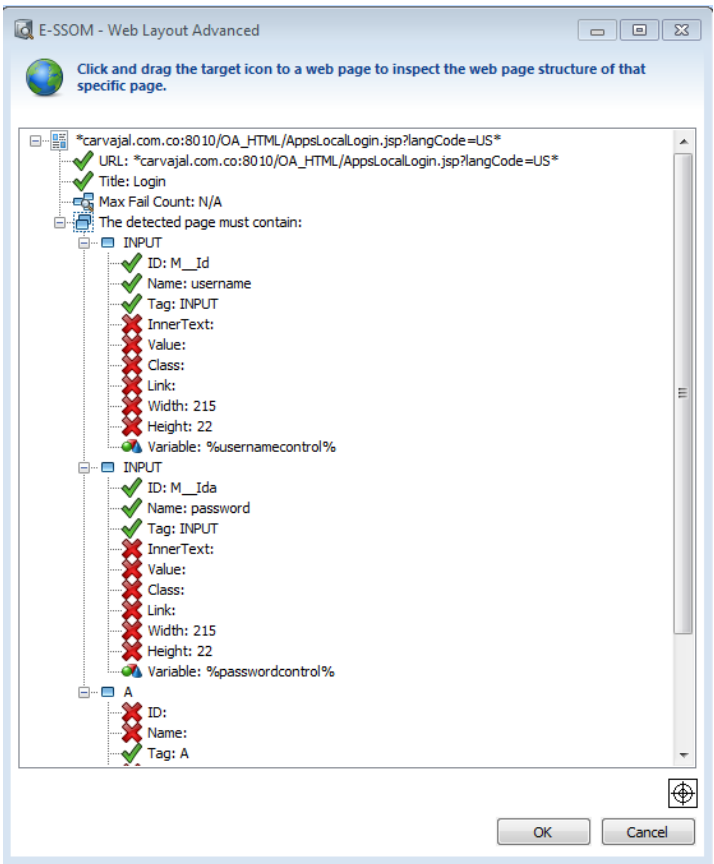


Figura 3.29: Ícono “objetivo” para realizar la virtualización

Se realizaron pruebas con un grupo de usuarios a los cuales se les instaló el software en sus respectivos equipos para más adelante comparar resultados.

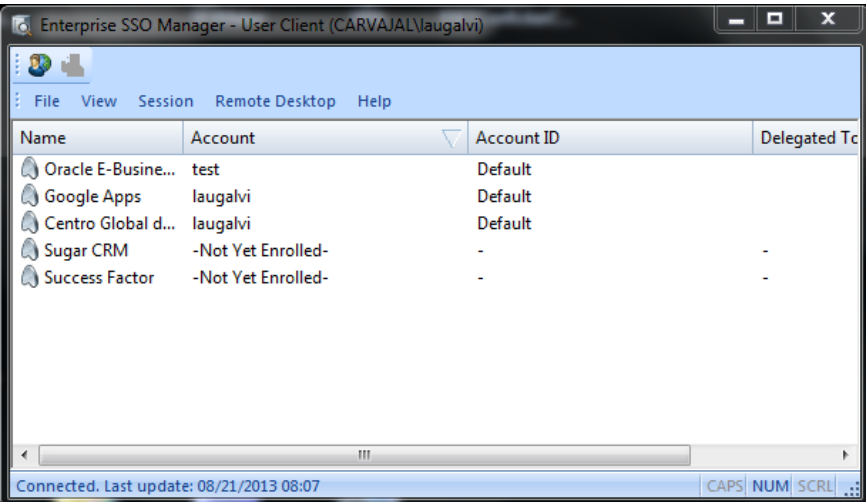


Figura 3.30: Cliente usuarios finales

3.4 Pruebas

3.4.1 Pruebas de usabilidad

La prueba de usabilidad se basó en un caso de estudio con un flujo de actividades para el uso de las dos aplicaciones, como se muestra en la tabla 3.4 y la tabla 3.5.

E-SSOM

Paso #	Descripción
1	Ingrese al correo corporativo Google Apps
2	Ingrese credenciales incorrectas y verifique que de nuevo le pide ingresar las credenciales correctas
3	Ingrese las credenciales correctas para la aplicación
4	Ingrese a la aplicación SugarCRM
5	Ingrese credenciales incorrectas y verifique que de nuevo le pide ingresar las credenciales correctas
6	Ingrese las credenciales correctas para la aplicación
7	Ingrese a la aplicación Oracle E-bussiness suite
8	Ingrese credenciales incorrectas y verifique que de nuevo le pide ingresar las credenciales correctas
9	Ingrese las credenciales correctas para la aplicación
10	Ingrese a la aplicación Success Factors
11	Ingrese credenciales incorrectas y verifique que de nuevo le pide ingresar las credenciales correctas
12	Ingrese las credenciales correctas para la aplicación
13	Ingrese al portal del Centro global de atención
14	Ingrese credenciales incorrectas y verifique que de nuevo le pide ingresar las credenciales correctas
15	Ingrese las credenciales correctas para la aplicación
16	Ingrese al software E-SSOM (User Client)
17	“Elimine” las credenciales de la aplicación Oracle E-bussiness suite
18	Ingrese de nuevo a la aplicación Oracle E-bussiness suite
19	Ingrese las credenciales de nuevo a Oracle E-bussiness suite

Tabla 3.4: Caso de estudio, pruebas de usabilidad E-SSOM

Una vez aplicado el caso de estudio se lleva a cabo la siguiente encuesta de usabilidad:

1. En una escala de 1 a 5, donde 1 es “muy difícil” y 5 es “muy fácil” ¿Cómo estuvo el proceso para ingresar a las aplicaciones con el nuevo software?
2. Percepción en cuanto al nuevo software: ¿“muy útil”, “útil”, “bueno”, “necesario” o “nada útil”?
3. ¿Necesitó alguna ayuda técnica para realizar el proceso de ingreso a las aplicaciones?
4. ¿Encontró fácilmente las funcionalidades requeridas?

- (a) La mayoría de los pasos
- (b) En algunos pasos
- (c) Ninguno de los pasos

5. En una escala de 1 a 5, donde 1 es “muy difícil” y 5 es “muy fácil” ¿Cómo considera el proceso para cambiar las credenciales de las aplicaciones?

Metapass SSO

Paso #	Descripción
1	Ingresa a la aplicación Metapass SSO
2	Ingresa al portal de la cooperativa
3	Ingresa al portal del colaborador
4	Ingresa a la aplicación E-bussiness suite
5	Ingresa al correo corporativo
6	Ingresa a la aplicación Success Factors
7	Ingresa al portal del centro global de atención de atención
8	Cambia las credenciales del portal del colaborador por unas incorrectas
9	Ingresa de nuevo al portal del colaborador y verifique que no le permita ingresar al portal del colaborador
10	Cambia las credenciales e ingresa las credenciales correctas en el portal del colaborador
11	Ingresa de nuevo al portal del colaborador y verifique que le permite ingresar al portal del colaborador

Tabla 3.5: Caso de estudio, pruebas de usabilidad Metapass SSO

Una vez aplicado el caso de estudio se lleva a cabo la siguiente encuesta de usabilidad:

1. En una escala de 1 a 5, donde 1 es “muy difícil” y 5 es “muy fácil” ¿Cómo estuvo el proceso para ingresar a las aplicaciones con el nuevo software?
2. Percepción en cuanto al nuevo software: ¿“muy útil”, “útil”, “bueno”, “necesario” o “nada útil”?
3. ¿Necesitó alguna ayuda técnica para realizar el proceso de ingreso a las aplicaciones?
4. ¿Encontró fácilmente las funcionalidades requeridas?
 - (a) La mayoría de los pasos
 - (b) En algunos pasos
 - (c) Ninguno de los pasos
5. En una escala de 1 a 5, donde 1 es “muy difícil” y 5 es “muy fácil” ¿Cómo considera el proceso para cambiar las credenciales de las aplicaciones?

Esta prueba se aplicó en un contexto real, con un determinado grupo de usuarios los cuales la respondieron y en base a esta se pudo obtener una buena apreciación de las dos herramientas para posteriormente tenerlo en cuenta con cualquier decisión que se tome.

De las pruebas de usabilidad realizadas se obtuvieron los siguientes resultados, representados estadísticamente:

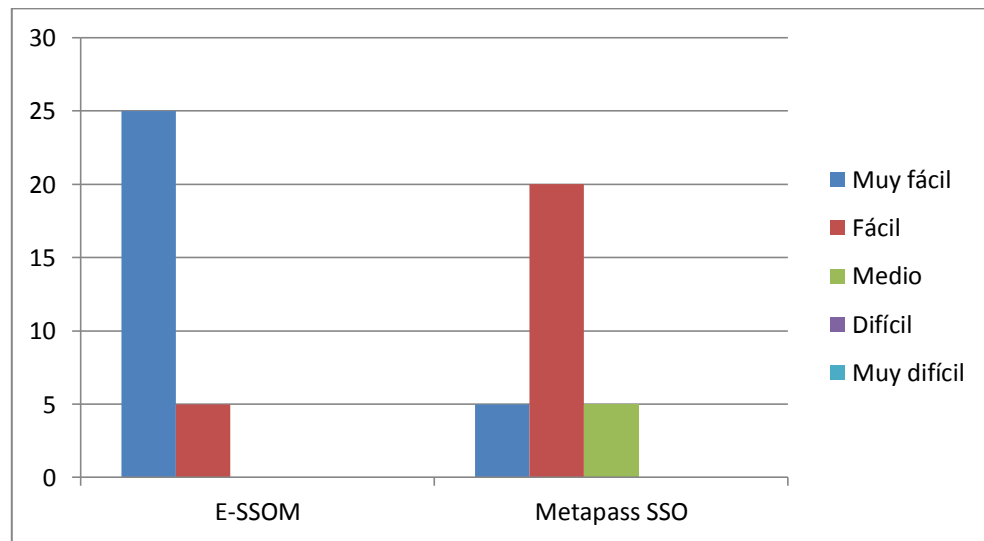


Gráfico 3.4: Proceso de ingreso a las aplicaciones

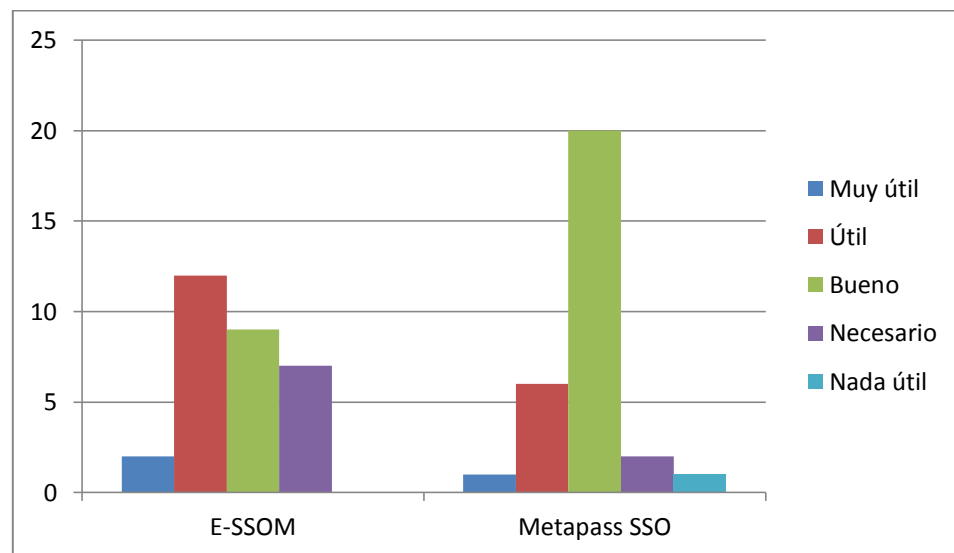


Gráfico 3.5: Percepción del software

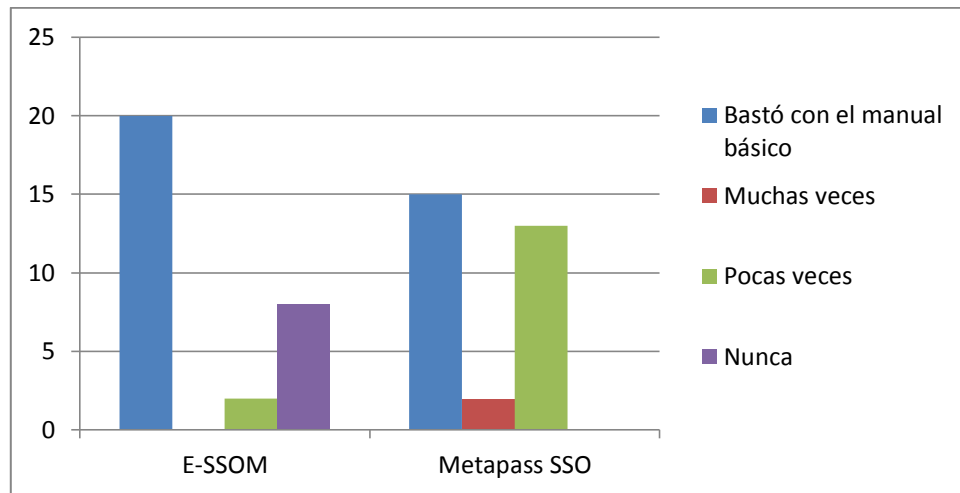


Gráfico 3.6: Necesidad de ayuda técnica

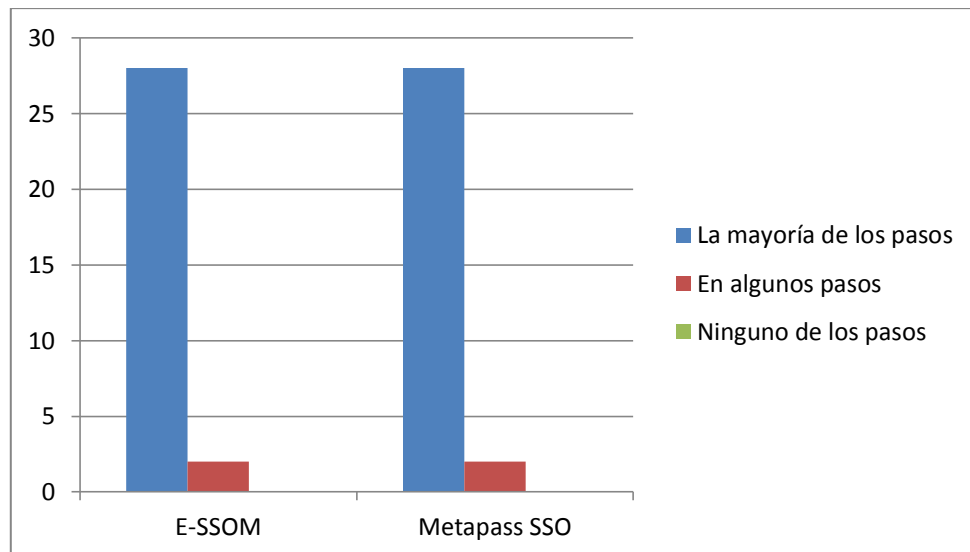


Gráfico 3.7: Encontrar las funcionalidades requeridas

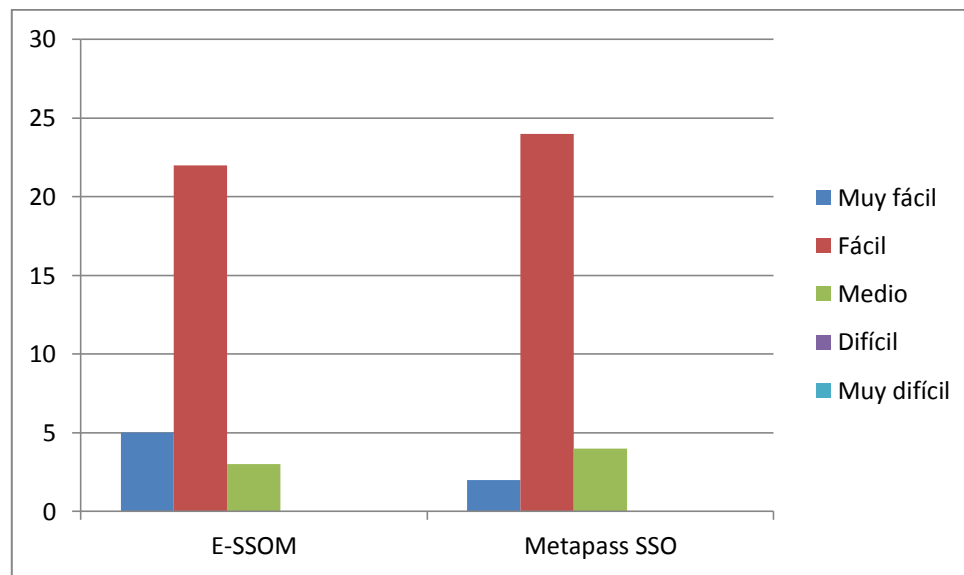


Gráfico 3.8: Proceso para cambiar credenciales

3.4.2 Pruebas alfa y beta

La prueba alfa se llevó a cabo por dos personas con conocimientos técnicos, fueron hechas en ambas herramientas (Metapass SSO y E-SSOM), las pruebas fueron tipo “caja negra” definiendo entradas y salidas para cada una de las herramientas. Esta prueba se llevó a cabo en la primera fase de implementación de las herramientas por lo cual se llamó “alfa”.

Se realizaron pruebas de caja negra ya que fueron basadas en la especificación externa del software, con estos resultados se pudo analizar que tanto cumplían las aplicaciones con los requisitos de la empresa.

En esta prueba se encontraron algunos inconvenientes, en cuanto a la herramienta Metapass SSO en algunos momentos la aplicación se volvía lenta debido al launchpad desde el cual se abren las aplicaciones, no iniciaba automáticamente al encender el equipo, la aplicación CGA (Centro Global de Atención) abría en el idioma Portugués sin dar la opción de cambiarlo al idioma Español.

En cuanto a la herramienta E-SSOM aunque funcionaba correctamente en el navegador Internet Explorer no funcionaba correctamente en el navegador Chrome, la aplicación CGA no permitía escoger el idioma.

La prueba beta se llevó a cabo por un grupo de usuarios finales, también pruebas tipo “caja negra”, donde los usuarios registraron los problemas encontrados durante el uso de las herramientas, para luego estudiar los resultados y finalmente analizar el cumplimiento de los requerimientos que tenía la empresa. Esta prueba se realizó en la última fase de la implementación de las herramientas (Metapass SSO y E-SSOM), por lo cual se llamó “beta”.

En esta prueba ya los inconvenientes vistos en la anterior prueba, en su mayoría estaban resueltos, en cuanto a los problemas presentados con Metapass SSO se lanzó un script vía

GPO por medio del directorio activo para que la aplicación iniciara automáticamente, funcionó con algunos usuarios debido a permisos en los equipos. Se solucionó la opción del idioma en la aplicación CGA modificando el flujo de trabajo de la aplicación.

En cuanto a los problemas presentados con E-SSOM se actualizó el plugin *chromeextension.crx* funcionando correctamente en el navegador Chrome, también se configuró la aplicación CGA para que permitiera escoger el idioma.

Capítulo 4

Conclusiones

En este capítulo se presentan las conclusiones del trabajo de grado con respecto a los objetivos cumplidos y en general con el proceso de desarrollo en la modalidad práctica como trabajo de grado.

La implementación de un sistema Single Sign On representa una verdadera ayuda para una empresa, ya que de los usuarios que participaron en las pruebas sus llamadas a la mesa de ayuda disminuyeron para casos de olvido de usuario o contraseña, por lo tanto se puede disminuir el número de peticiones y aumentar la productividad donde el tiempo en el que se atendían estas peticiones se emplee en otros casos.

La seguridad también se ve incrementada ya que el servidor SSO es el único punto que acepta credenciales.

Con las pruebas alfa y beta que se realizaron se pudo establecer si las aplicaciones cumplían con los requisitos de la empresa o al menos en gran parte, se pudo concluir que la herramienta METAPASS SSO tuvo falencias en cuanto los usuarios finales la probaron, al tener un launchpad la hace un poco lenta y ciertos casos se perdía la conexión obligando a ingresar de nuevo mediante el launchpad, algunos usuarios presentaron problemas en el momento de la autenticación, no iniciaba automáticamente y era un requisito que solicitaban la mayoría de los usuarios.

En cuanto a la herramienta E-SSOM, al principio funcionaba mal en el navegador Chrome y al ser este el navegador que la mayoría de los usuarios utiliza en la empresa era vital que tuviera un buen funcionamiento, problema que se solucionó para que funcionara correctamente, mediante la actualización del plugin de E-SSOM para Chrome.

En cuanto a los objetivos, las dos herramientas los llevan a cabo, cada una de ellas maneja una arquitectura propia para la estructura de la empresa y se relacionan con el directorio activo que se tiene de una manera correcta.

Que la herramienta cumpla con la mayoría de los requerimientos principales y funcione de manera correcta, además de ser útil para los usuarios y que ayude a disminuir las peticiones a la mesa de ayuda es lo más importante a la hora de escogerla, sabiendo que va a representar un beneficio que compensa lo invertido.

Al realizar la práctica en la empresa Carvajal S.A. fue un primer paso para incursionar en el ámbito laboral, permitió ver de cerca cómo funciona una empresa, aprender en un entorno real y por supuesto adquirir nuevas habilidades.

Referencias

- [1] D. Garlan and M. Shaw. *An Introduction to Software Architecture*. Carnegie Mellon University, 1994.
- [2] Directorio Activo, “Qué es un directorio activo,” [Online]. Available: <http://www.ordenadores-y-portatiles.com/directorio-activo.html>, Consultado el 4 de febrero de 2013.
- [3] I. M. Caballero and J. Cano. “Consideraciones para implementar una arquitectura Single Sign On,” Universidad de los Andes, Bogotá, Colombia, 2003.
- [4] MIT Kerberos Consortium. Documentation. [Online]. Available: <http://www.kerberos.org/docs/index.html>, Consultado el 5 de febrero de 2013.
- [5] Visual Guard. “Single Sign-on e integración con el Active Directory”. [Online]. Available: <http://www.visual-guard.com/SP/>, Consultado el 6 de febrero de 2013.
- [6] OneSign Single Sign-On. “User Authentication Solution”. [Online]. Available: <http://www.imprivata.com/products-and-solutions>, Consultado el 11 de febrero de 2013.
- [7] ESSO Suite. Oracle. [Online]. Available: <http://www.oracle.com>, Consultado el 12 de febrero de 2013.
- [8] Evidian Enterprise SSO. Evidian. [Online]. Available: <http://www.evidian.com/iam/enterprise-ssol/>, Consultado el 13 de febrero de 2013.
- [9] Crowd: Identity manager for web apps. Crowd Atlassian. [Online]. Available: <https://www.atlassian.com/software/crowd/overview>, Consultado el 18 de febrero de 2013.
- [10] PingFederate. Ping Identity. [Online]. Available: <https://www.pingidentity.com/products/pingfederate/>, Consultado el 19 de febrero de 2013.
- [11] SecureLogin. NetIQ. [Online]. Available: <https://www.netiq.com/products/securelogin/>, Consultado el 20 de febrero de 2013.
- [12] Enterprise Single Sign-on (Quest). Dell Software. [Online]. Available: <http://www.quest.com/esso/>, Consultado el 25 de febrero de 2013.
- [13] TrustBroker Security Solutions. TrustBroker. [Online]. Available: <https://sap.cybersafe.com/>, Consultado el 26 de febrero de 2013.

[14] Passlogix. Passlogix. [Online]. Available: <http://www.oracle.com/us/corporate/acquisitions/passlogix/index.html>, Consultado el 27 de febrero de 2013.

[15] Seguridad y algoritmos de encriptación. Cryptoforge. [Online]. Available: <http://www.cryptoforge.com.ar/seguridad.htm>, Consultado el 4 de marzo de 2013.

[16] Extensible Markup Language. Wikipedia. [Online]. Available: http://es.wikipedia.org/wiki/Extensible_Markup_Language, Consultado el 1 de abril de 2013.

[17] Directorio Activo (AD). Microsoft. [Online]. Available: http://www.microsoft.com/spain/windowsserver2008/roles/apps_ad.msp, Consultado el 7 de mayo de 2013.

[18] Windows Data Protection. Microsoft. [Online]. Available: <http://msdn.microsoft.com/en-us/library/ms995355.aspx>, Consultado el 2 de julio de 2013 y el 5 de agosto de 2013.

[19] Microsoft SQL Server. Microsoft. [Online]. Available: http://es.wikipedia.org/wiki/Microsoft_SQL_Server, Consultado el 3 de julio de 2013 y el 12 de agosto de 2013.

[20] Descripción del cifrado de datos transparente (TDE). Microsoft. [Online]. Available: [http://technet.microsoft.com/es-es/library/bb934049\(v=sql.100\).aspx](http://technet.microsoft.com/es-es/library/bb934049(v=sql.100).aspx), Consultado el 15 de julio de 2013.

[21] Microsoft. Configuración de windows server 2008 Active Directory, Exámen 70 640. [Libro Digital], Consultado el 4 de febrero de 2013 y el 24 de junio de 2013.

[22] Download Metapass. Sourceforge. [Online]. Available: <http://sourceforge.net/projects/metapass/>

[23] Enterprise Single Sign On Manager E-SSOM. Tools4ever. [Online]. Available: <http://www.tools4ever.com/software/enterprise-single-sign-on-manager/>

ANEXOS

Anexo A: Especificación de requerimientos

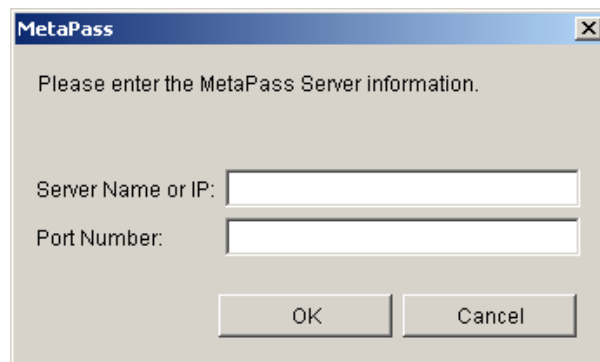
	Especificación de Requerimientos ISO-9000 Universidad del Valle	Documento: ER-001	Revisión: 001
SISTEMA CENTRALIZADO DE AUNTENTICACIÓN Y AUTORIZACIÓN “SINGLE SIGN ON”			Fecha:
1. Modulo Usuarios			
Req.	Descripción		
R 1.1	El sistema en el módulo usuarios, deberá permitir la validación de usuarios con el directorio activo de la empresa (Windows server 2008)		
R 1.2	El sistema deberá permitir que los usuarios puedan acceder a las aplicaciones de acuerdo a los permisos que tengan.		
R 1.3	Los usuarios deben autenticarse una vez a cada aplicación a la que tengan permisos.		
R 1.4	Si el usuario ingresa la contraseña errónea a la aplicación, el sistema debe volver a pedirle la contraseña.		
R 1.5	Al usuario autenticarse a las aplicaciones, las credenciales deben ser encriptadas bajo algún algoritmo para aumentar la seguridad		
2. Modulo Aplicaciones			
Req.	Descripción		
R 2.1	El sistema deberá permitir la conexión con Oracle E-Business Suite		
R 2.2	El sistema deberá permitir la conexión con el Portal de Success Factors		
R 2.3	El sistema deberá permitir la conexión con el Portal del Centro Global de Atención		
R 2.4	El sistema deberá permitir la conexión con Google Apps		
R 2.5	El sistema deberá permitir la conexión con el portal SugarCRM		
R 2.6	Cuando cada aplicación exija cambio de contraseña, el sistema debe tener la opción de que se le cambie la contraseña al usuario sin necesidad de involucrarlo (que sea transparente al usuario) y pueda seguir ingresando a las aplicaciones.		
3. Modulo Administrador			
Req.	Descripción		
R 3.1	El sistema debe permitir al administrador manejar la conexión al servidor de la aplicación		
R 3.2	El sistema deberá permitir al administrador integrar nuevas aplicaciones al sistema		
R 3.3	El sistema deberá permitir al administrador crear los scripts para cada una de los eventos		

	que se ejecutan con cada aplicación
R 3.4	El sistema deberá permitir al administrador crear grupos de usuarios
R 3.5	El sistema deberá permitir al administrador modificar los grupos de usuarios
R 3.6	El sistema deberá permitir al administrador crear políticas para definir permisos por grupos de usuarios
R 3.7	El sistema deberá permitir al administrador modificar las políticas de usuario

Anexo B: Guía de instalación Metapass SSO

PROCESO DE INSTALACIÓN

1. Ingresar en el equipo con privilegios de administrador.
2. Dar doble click en el archivo Metapass_SSO_Setup.msi para iniciar el proceso de instalación.
3. Seguir las instrucciones en pantalla a través del proceso de instalación (típica).
4. La primera vez que inicies SSO Desktop, aparecerá la siguiente ventana para ingresar la información del servidor.



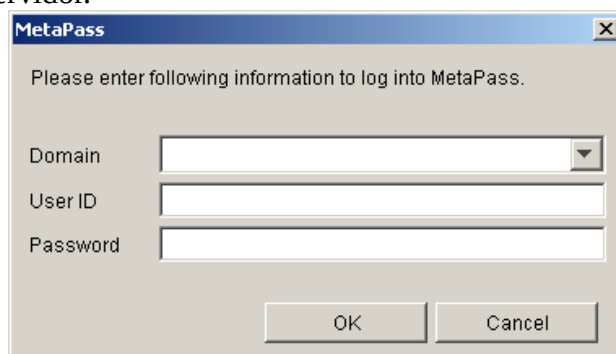
A screenshot of a Windows-style dialog box titled "MetaPass". The text inside says "Please enter the MetaPass Server information." There are two input fields: "Server Name or IP:" and "Port Number:". Below the fields are two buttons: "OK" and "Cancel".

Deberás ingresar la siguiente información

- Server Name or IP: CTSSSOBOG01
- Port Number: 6000

Click en OK.

5. Deberá aparecer la siguiente ventana de autenticación que indicará que se realizó la conexión con el servidor.



A screenshot of a Windows-style dialog box titled "MetaPass". The text inside says "Please enter following information to log into MetaPass." There are three input fields: "Domain" (with a dropdown arrow), "User ID", and "Password". Below the fields are two buttons: "OK" and "Cancel".

Escoge el dominio:



A screenshot of the MetaPass login dialog box. The title bar says 'MetaPass'. The text inside says 'Please enter following information to log into MetaPass.' There are three input fields: 'Domain' with a dropdown menu showing 'CARVAJAL.COM.CO', 'User ID' with an empty text box, and 'Password' with an empty text box. At the bottom are 'OK' and 'Cancel' buttons.

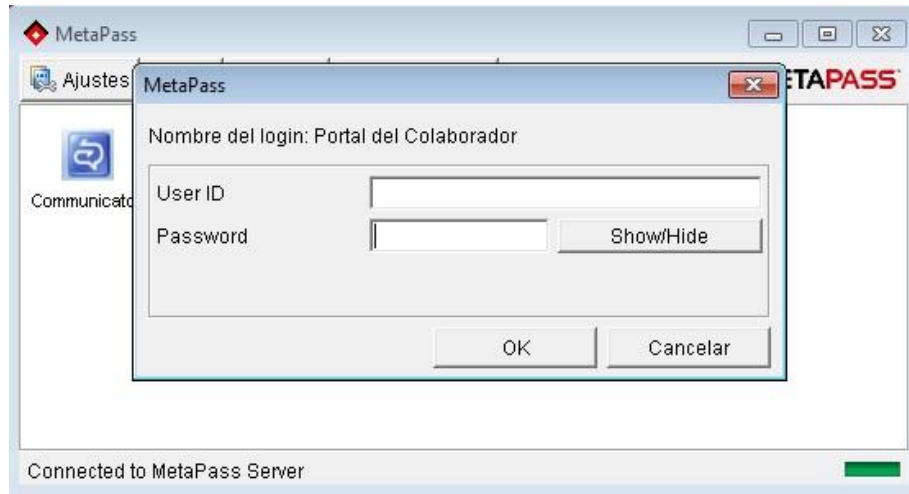
E ingresa con tu usuario de dominio y contraseña.

6. Finalmente, aparecerá la ventana principal si el usuario ha sido autenticado exitosamente.



USO BÁSICO DEL APLICATIVO

1. Al hacer click en una aplicación, aparecerá la siguiente ventana de login, ingresar con las credenciales propias para cada aplicación y hacer click en OK.



2. Se abrirá la aplicación, y metapass se logueará con las respectivas credenciales.
3. El usuario y la contraseña de cada aplicación quedará guardada en Metapass.

Anexo C: Guía de instalación E-SSOM

GUÍA DE INSTALACIÓN

Instalando el Software Cliente E-SSOM

El Software Cliente E-SSOM debe ser instalado en los clientes que deseen loguearse a las aplicaciones automáticamente. El Software Cliente E-SSOM puede ser instalado manualmente o vía GPO.

Instalación Manual

El Software Cliente E-SSOM puede ser instalado manualmente para propósitos de prueba.

Nota: La cuenta que es usada para instalar el Software Client E-SSOM debe tener derechos administrativos sobre la máquina en la cual va a ser instalado el software.

1. Navegue hacia el directorio que contiene el software los archivos de instalación de E-SSOM Software Client. Estos son instalados por defecto en 'C:\Program Files\Tools4ever\SSO\Admin Console\SSO Client Software'.
2. Corra el ejecutable 'SSOSetClientReg.exe' para colocar las entradas del registro que serán usadas en el software cliente para localizar el E-SSOM Central Service.

E-SSOM - Set Client Registry Settings

Use this dialog to set the client registry settings manually.

SSO Client Service

Server Names:

Port Number:

Log Location:

Max Log Size: MB

Events to Log: ☐ Error ☐ Debug ☐ Info

SSO Hook

Log Location:

Max Log Size:

Events to Log: ☐ Error ☐ Debug ☐ Info

SSO Client

Log Location:

Max Log Size:

Events to Log: ☐ Error ☐ Debug ☐ Info

SSO Helper

Log Location:

Max Log Size:

Events to Log: ☐ Error ☐ Debug ☐ Info

3. Ingrese el nombre del servidor en el cual corre el E-SSOM Central Service y el número del puerto usado para comunicarse con el servicio. (Por defecto 36785).
4. Click en 'Save'.
5. Click en 'Close' para cerrar la herramienta 'Set Client Registry Settings'.
6. Instalar el software E-SSOM Client ejecutando el paquete 'SSOUserSoftware.msi'.

Después de instalar el paquete, el E-SSOM User Client puede ser iniciado desde el menú 'Start'. (Localización por defecto: Start -> All Programs -> Tool4ever -> E-SSOM -> User Client -> User Client)

USO BÁSICO DEL APLICATIVO

ENTERPRISE SINGLE SIGN ON MANAGER (E-SSOM)

Antes de empezar debes saber que las aplicaciones incluidas en este piloto son 5:

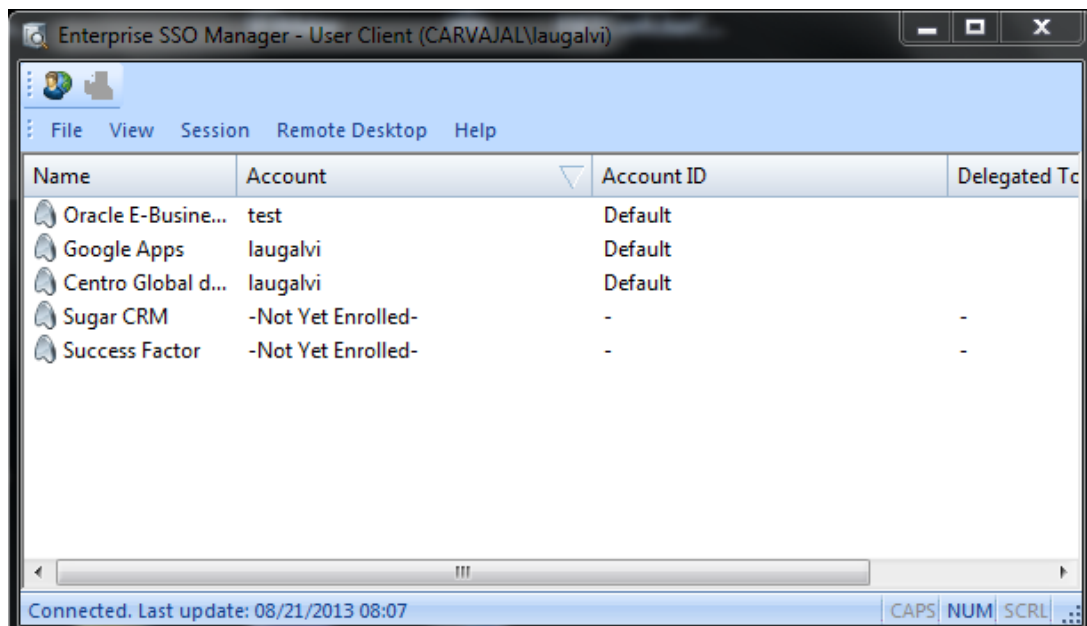
- Google Apps
- Centro Global de Atención (CGA)
- SugarCRM
- Success Factor
- Oracle E-business Suite

USO DEL APLICATIVO E-SSOM

1. En la parte inferior derecha se encuentra el ícono de la aplicación.



2. Hacer doble click para asegurar que está correcta la aplicación.



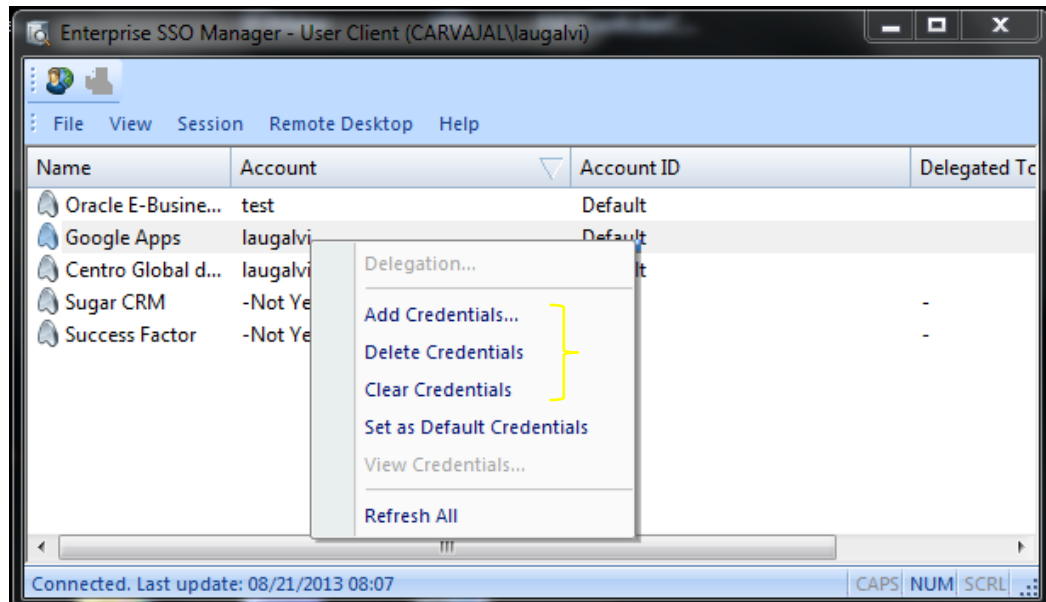
Encontrará tres (3) columnas: Name, Account y Account ID.

En la columna **Name** están las aplicaciones que están funcionando en el software.

En la columna **Account** están los nombres de usuario que tienes para cada una de las respectivas aplicaciones. Si aparece **-Not yet enrolled-** significa que aún no has ingresado tus credenciales.

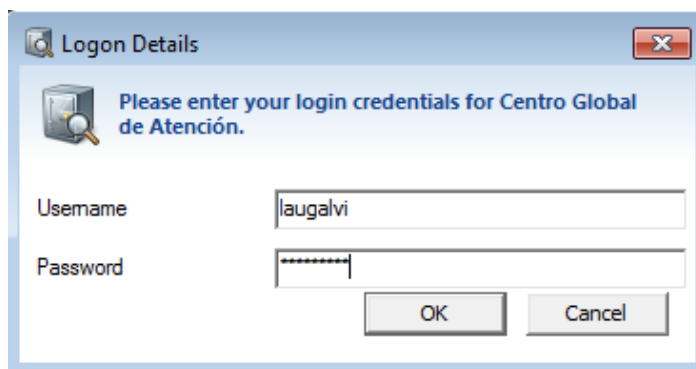
En la columna **Account ID** son las credenciales para cada aplicación, controlando cuales están funcionando. Si ves **Default** significa que ya ingresaste tus credenciales.

3. Hacer click derecho en el nombre de usuario y encontrará las siguientes opciones.



Con las opciones Add Credentials, Delete Credentials y Clear Credentials podrás modificar tus credenciales.

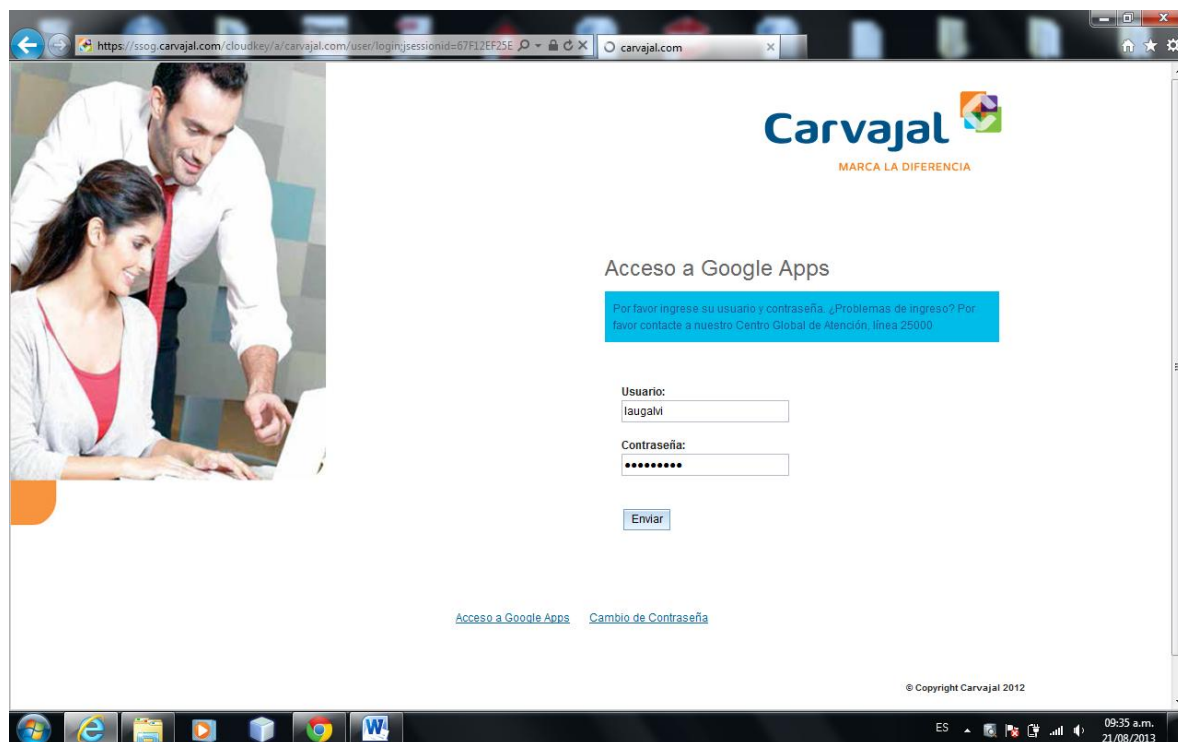
4. Cuando inicie alguna de las aplicaciones, si no se han ingresado credenciales, aparecerá esta pantalla en la cual debes ingresar tus credenciales.



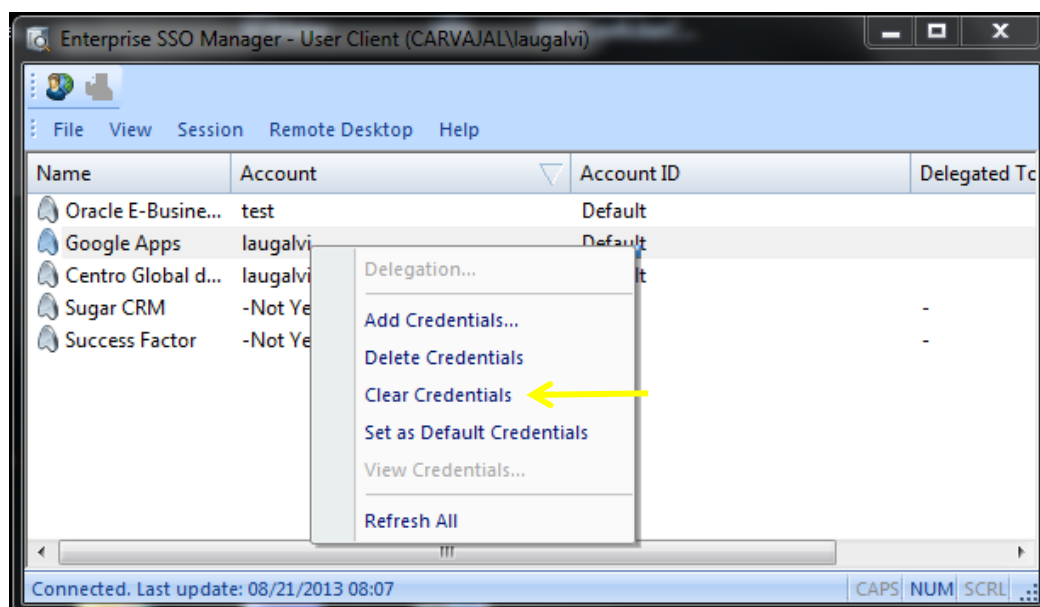
Hacer click en OK y se ingresará a la aplicación.

5. La próxima vez que ingreses a la aplicación será automáticamente, sin necesidad de ingresar credenciales.

Nota: Por seguridad las credenciales no quedan guardadas en el navegador.



6. Cuando alguna de tus contraseñas cambie, deberás ir a la opción **Clear Credentials** e ingresar la nueva contraseña:



7. Ahora puedes empezar a usar E-SSOM y experimentar el proceso de Single Sign On.