3. SSO

3.1 EL CONCEPTO DE SINGLE SIGN-ON

El concepto de Single Sign-On se refiere al acceso a múltiples recursos por medio de un único proceso de ingreso o autenticación. Muchas 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. [3]

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 solo existe un único punto de autenticación y registro en el sistema.

Uno de los beneficios de una arquitectura Single Sign-On, es que los usuarios deben autenticarse una sola vez. En cambio al concentrarse la seguridad en un único punto, debemos extremar la misma.

Single Sign-On no se refiere necesariamente a una sincronización de *password*, ya que en ese caso todas las aplicaciones y servicios funcionan con el mismo. No puede considerarse tampoco una implementación real, ya que en lugar de fortalecer las características de seguridad del sistema, éstas se estarían debilitando, ya que se corre el riesgo de que si un intruso logra conseguir el *password* de una de las aplicaciones o servicios, inmediatamente tendrá acceso a todas ellas.

Una implementación real de SSO, deberá almacenar en una base de datos los *username* y *password* que le permiten al usuario acceder a cada una de las aplicaciones, ya que el proceso de *login* se realiza de manera transparente para el usuario, una vez que éste ha sido autenticado por medio de la arquitectura SSO.

3.2 ARQUITECTURA

En la siguiente imagen se muestra como es la arquitectura de una aplicación que implementa single sign-on.

Si no estuviera implementada la SSO, si el usuario quiere acceder a distintas aplicación, cada una de ellas le pedirá que introduzca sus credenciales, es decir, su usuario y password correspondientes.

Para evitar lo indicado en el párrafo anterior, el usuario introduce los datos de acceso a la aplicación SSO y el agente SSO consultará la base de datos correspondiente a los datos de acceso de la aplicación solicitada, y actuará en consecuencia dando o no permiso para acceder en función de si dispone de la información necesaria o no.

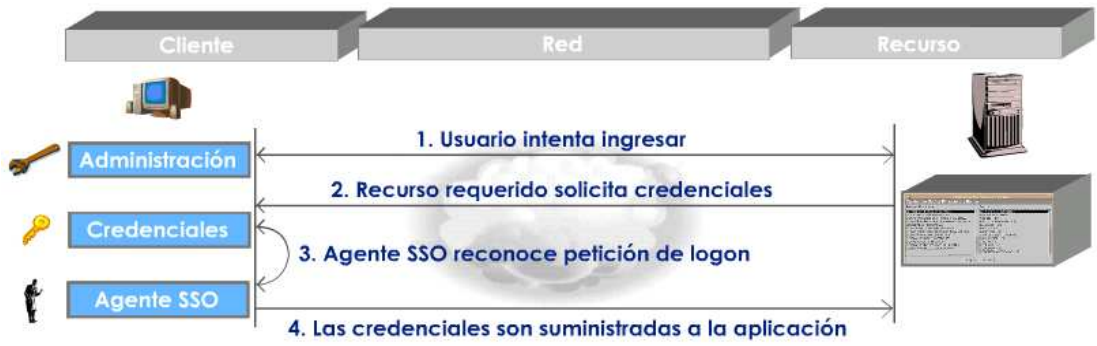

Imagen 1 - Arquitectura Single Sign-On

3.3 REQUISITOS

Para el desarrollo de la aplicación single sign-on es necesario disponer de una base de datos donde se almacene toda la información relativa a los usuarios que hay en el sistema y sus aplicaciones.

Junto con esta información debemos guardar para cada aplicación el usuario y password correspondiente para que al pinchar en el enlace de la aplicación, el acceso sea transparente al usuario sin necesidad de introducir ningún dato.

Otro de los requisitos para que la aplicación funcione correctamente, es que el administrador encargado de dar de alta las aplicaciones sea personal cualificado, ya que para poder hacer el acceso de forma transparente al usuario, debe saber cómo es la cadena de login de la aplicación en cuestión y componer la url de la aplicación que se le mostrará al usuario.

Un ejemplo de lo anterior seria:

http://waine.us.es/~mhervas/wsso/login.php?username=%u&password=%p

En esta línea el administrador debe de saber que la aplicación, en este caso la propia aplicación SSO, tiene como parámetros de acceso las cadenas "username" y "password" que previamente ha debido de buscar en el código de la aplicación.