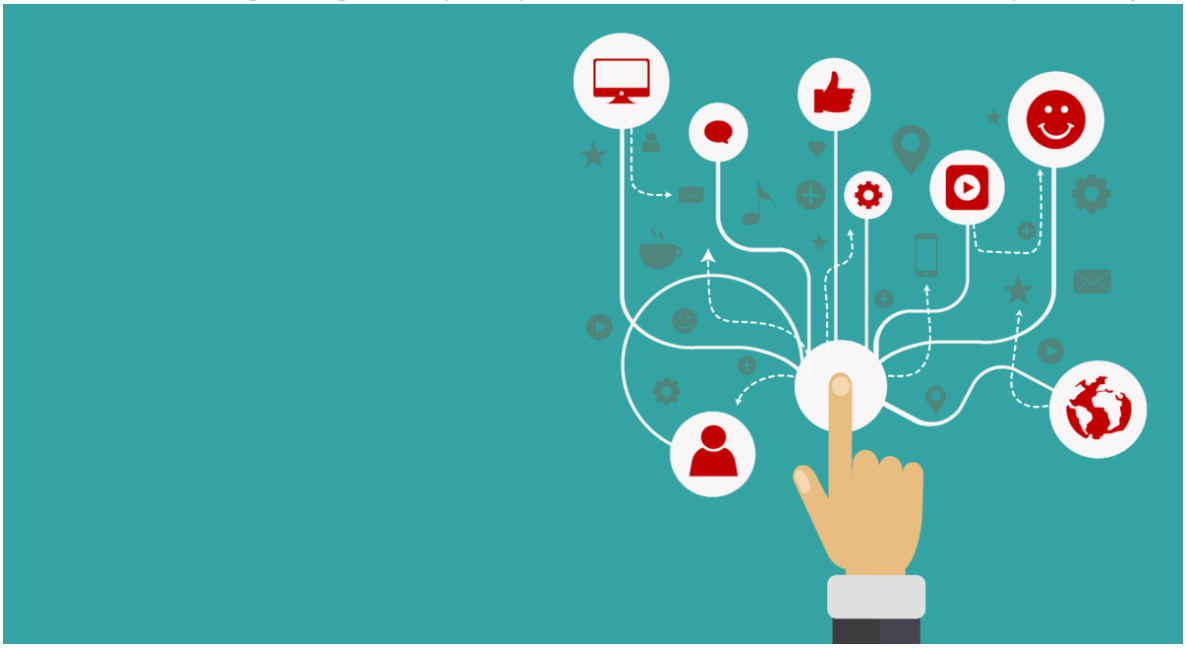
CHAKRAY

¿Qué es el Single Sign on (SSO)? Definición, características y ventajas



Cada vez, utilizamos más sistemas en nuestro día a día y memorizar las complejas contraseñas de cada uno de estos sistemas es un reto al que muchos usuarios se enfrentan día a día. El Single Sign On (SSO) puede ser la solución a esta problemática, gracias a ella podremos acceder a diferentes aplicaciones y servicios con una única identidad y nos facilitará el dar de alta y de baja a los usuarios en nuestros sistemas.

¿Qué es Single Sign On (SSO) y para qué sirve?

Single Sign On conocido también como **SSO** por sus siglas en inglés permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes sistemas y recursos. El SSO es de gran utilidad cuando existen diferentes sistemas a los que es posible acceder mediante una única contraseña y se desea evitar el ingreso repetitivo de estas cada vez que el usuario se desconecte del servicio. Para los usuarios supone una gran comodidad ya que identificándose solo una vez es posible mantener la sesión válida para el resto de las aplicaciones que hacen uso del SSO.

El SSO busca simplificar la experiencia de los usuarios en Internet facilitando las tareas de inicio de sesión completamente.

Con el sistema de identificación Single Sign On es posible a través de una cuenta tener múltiples accesos, por ejemplo ingresando a Gmail podemos acceder a sus diferentes utilidades web, como Google Docs, Google Maps, Google Books, etc.

Características de Single Sign On (SSO)

Este procedimiento de autenticación facilita las tareas de acceso a las diferentes plataformas, además cuenta con otras importantes características en aspectos de gestión sencilla, **seguridad**, facilidad de uso y transparencia.

Gestión sencilla

El uso de SSO realiza la sincronización de contraseñas e información del usuario, lo que proporciona la simplificación del acceso a los diferentes plataformas y recursos.

Seguridad

Este sistema de autenticación mejora la seguridad de la red y de las aplicaciones. Single Sign On puede identificar inequívocamente a un usuario por lo que cumple con normas más exigentes respecto a la seguridad.

La información proporcionada a SSO viaja cifrada por la red.

Facilidad de uso

Las soluciones SSO mejoran la experiencia del usuario evitando las interrupciones producidas por las solicitudes de contraseñas para acceder a sus herramientas informáticas.

El usuario se autentica una vez y el sistema le permite acceder los recursos para los cuales está autorizado.

Transparencia

El acceso a todas las aplicaciones por parte del usuario se realizan de forma transparente debido a la automatización del inicio de sesión.

Tipos de Single Sign On (SSO)

Empresa *single sign-on* (E-SSO)

Las empresas SSO están implementadas en ambientes de **integración de aplicaciones para empresas** (EAI, por sus siglas en inglés). Por lo tanto, simplemente con un conjunto de credenciales de inicio de sesión, se permite a los usuarios el acceso a todas las aplicaciones que están integradas en una empresa, existan o no ***on-premise*** o **en *cloud***.

Web *single sign-on* (Web-SSO)

Esta solución es perfecta para aplicaciones a las que se puede acceder a través de la web (sitios o servicios web), y su propósito es verificar la identidad de un usuario en diversas aplicaciones sin tener que identificarse repetidas veces. Tiene su base en un sistema de autenticación externa o de terceros.

Un servidor *proxy* SSO que ejecuta el sistema de autenticación, administra la información de acceso y lleva a cabo la confirmación de identidad antes de transferir los resultados al ordenador que gestiona el servicio o sitio web que lo ha solicitado. El servidor SSO y el servicio web se comunican a través de *tokens* de forma casi invisible para el usuario. Cuando el usuario está intentando registrarse en el sitio o servicio web, el sistema de autenticación genera un ***token* global** y envía el valor al usuario. Como consecuencia, el usuario puede introducir el *token* global en el sitio web que, a su vez, corrobora el valor con el sistema de autenticación para garantizar la identidad del usuario antes de concederle el acceso. Si el usuario ya está registrado en el sistema de autenticación, el servidor SSO transmite sus credenciales junto con un ***token* local** al sitio web, lo que significa que el acceso ha tenido éxito.

Identidad federada

El *Identity Management* federado (FIM, por sus siglas en inglés) o el SSO federado amplía el alcance de las tecnologías SSO estándar al unir diversas organizaciones bajo un sistema de autenticación. Mientras que el SSO tradicional permite el acceso a varios sistemas en una empresa, FIM lo permite dentro de **muchas empresas diferentes**. Sin embargo, ambos métodos autentican al usuario a través de una sola identidad.

Open ID

Como un enfoque descentralizado de las tecnologías SSO, *Open ID* funciona según el concepto de ***relying party*** (RP, en inglés) y de **proveedor de identidad** (IdP, en inglés). RP es el sitio web o servicio que desea autenticar al usuario, mientras que IdP lleva a cabo la autenticación al registrar la identidad elegida por el usuario (que se representa a través de un identificador URL que se llama *OpenID*). Las interacciones multipunto entre el usuario, el RP y el IdP ocurren a través de un agente de usuario como un navegador web.

OAuth

OAuth no es una tecnología en concreto, sino un estándar que está disponible para que todos lo implementen. Funciona según el principio ***token* de acceso** y puede ayudar a llevar a cabo el SSO. Un cliente o usuario interactúa con un s**ervidor de autenticación**para recibir un *token* de acceso que podría ayudarle a validar su identidad con un **servidor de recursos**. Los servidores de recursos se encargan de delegar un recurso a un cliente autorizado.

SSO con base en Kerberos

Este protocolo permite a los usuarios (el cliente) utilizar un ***ticket-granting ticket*** o un ***Ticket to Get Tickets*** (TGT) después de la verificación de sus credenciales. Un TGT se intercambia por un ***ticket* de servicio** del ***ticket-granting service*** (TGS). Los *tickets* de servicio permiten al usuario acceder a servicios que están protegidos en la red (por ejemplo, un servidor de correo).

Autenticación de tarjetas inteligentes

En vez de implantar un *software* para autenticar el mismo conjunto de credenciales como en los procesos SSO convencionales, los dispositivos *hardware* como las tarjetas inteligentes se pueden usar para conseguir resultados similares.

Lenguaje marcado para confirmaciones de seguridad (SAML)

El SAML es un estándar abierto con base en XML que puede potenciar las implementaciones SSO. Consta de dos partes, el proveedor de identidad (IdP) SAML y el proveedor de servicio (SP) SAML. Primero, el cliente o el usuario solicita conectarse al SP. A su vez, el SP solicita al IdP una aserción de autenticación. Una vez ésta emitida, el SP ofrece al usuario el servicio que necesita u opta por no hacerlo.

Ventajas y desventajas de Single Sign On (SSO)

Ventajas SSO	**Desventajas Single Sign On**
Acelera el acceso de los usuarios a sus aplicaciones.	Utilizar una única combinación aumenta las probabilidades de vulnerabilidad de contraseñas.
Reduce la carga de memorizar diversas contraseñas.	Al fallar SSO se pierde acceso a todos los sistemas relacionados.
Fácil de implementar y conectar a nuevas fuentes de datos.	Mayor riesgo de suplantación de identidad y fraude informático en accesos externos de usuario.

En el caso de las empresas contar con un sistema de autentificación como Single Sign On significa liberar al usuario de la carga de recordar numerosas contraseñas, además proporciona activos muy importantes relacionados directamente a la eficiencia, de esta manera es posible reducir la llamada al servicio de asistencia técnica o al departamento de informática para dar solución a los problemas originados por la seguridad de las contraseñas.