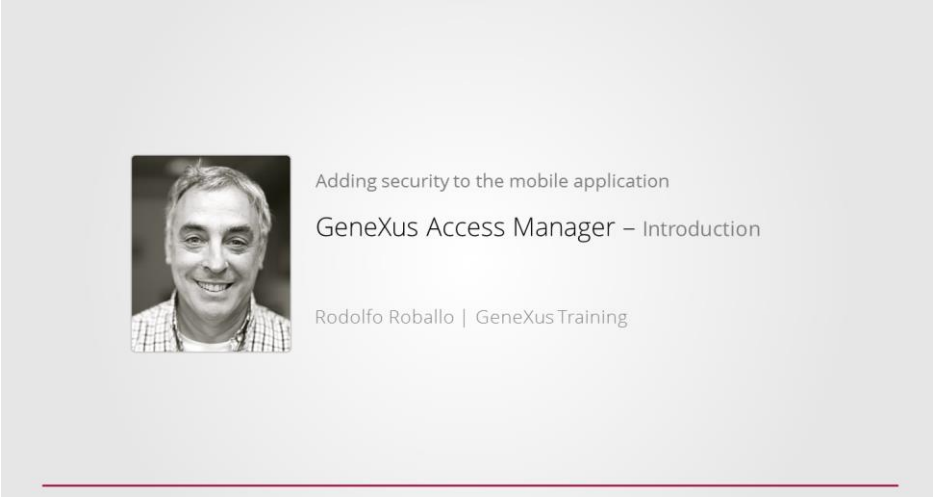
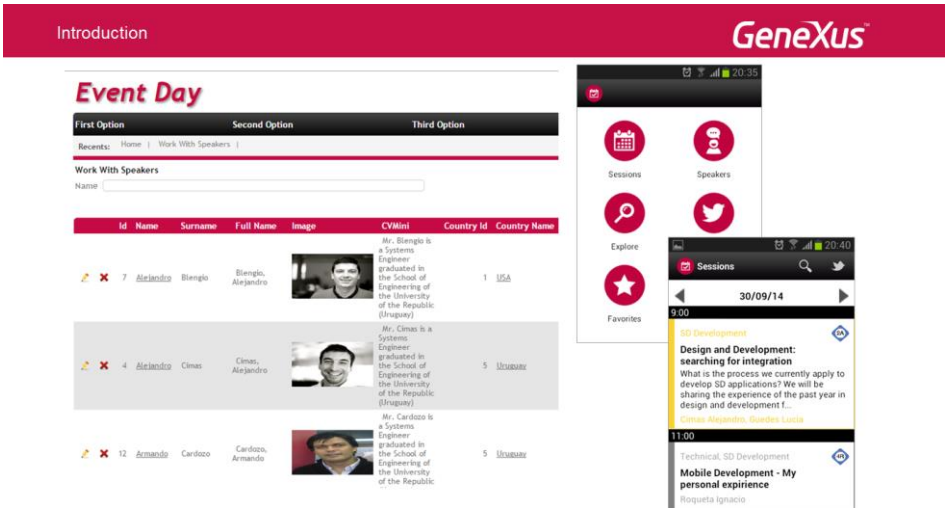
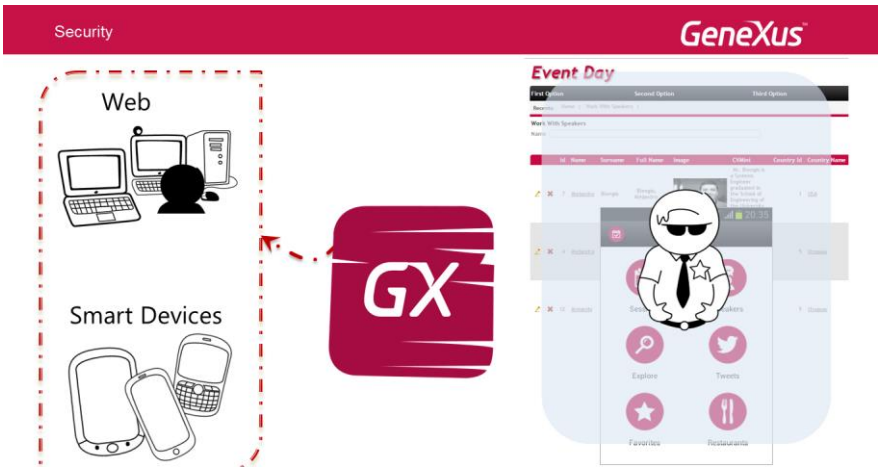
Introducción a GAM



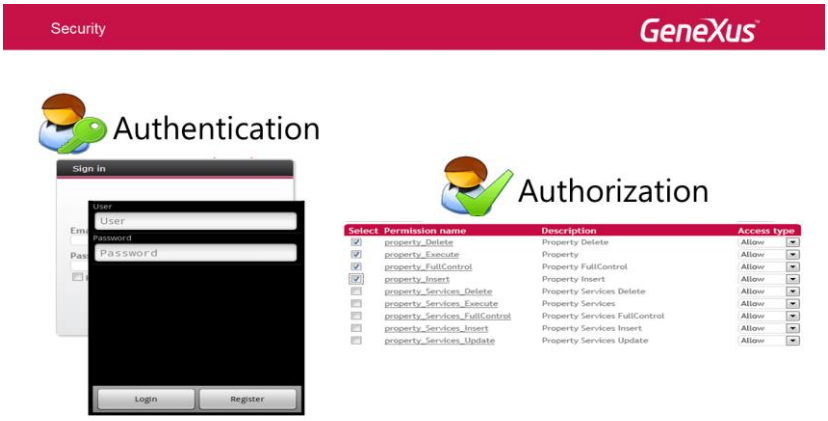
En videos anteriores hemos venido desarrollando una aplicación web y para dispositivos móviles para administrar los datos de un evento, con información de sus conferencias, oradores, etc.



Ahora queremos agregarle Seguridad a la aplicación, tanto a la parte web como a la de Smart Devices.

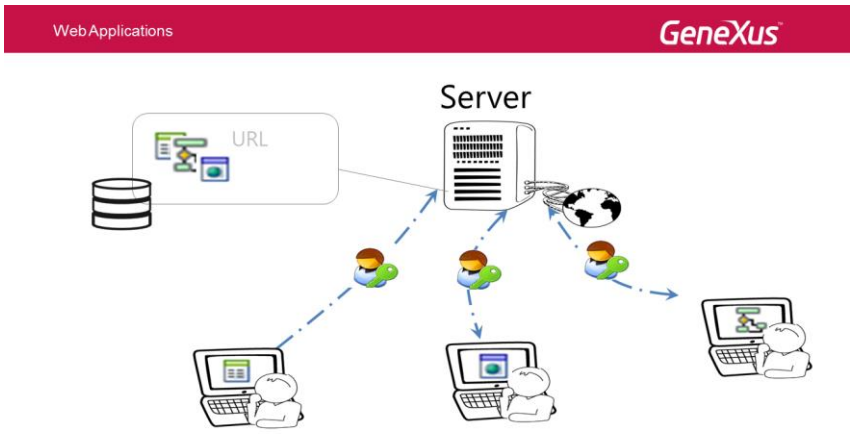


Esto significa asegurar que todos los usuarios que ingresen estén debidamente autenticados, (es decir, que el usuario sea quien dice ser); y autorizados, o sea que una vez que el usuario se autentica, se le permita el acceso o no a ciertas partes de la aplicación.



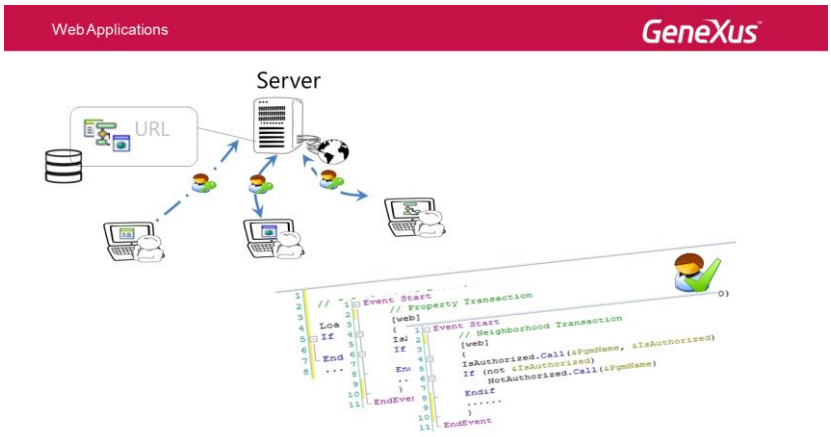
Veamos qué debe tener en cuenta el desarrollador GeneXus para implementar una solución al problema de la seguridad de las aplicaciones.

En el caso de las aplicaciones Web, como tienen varios puntos de entrada, cualquier objeto accesible por URL debe chequear permisos de autenticación.



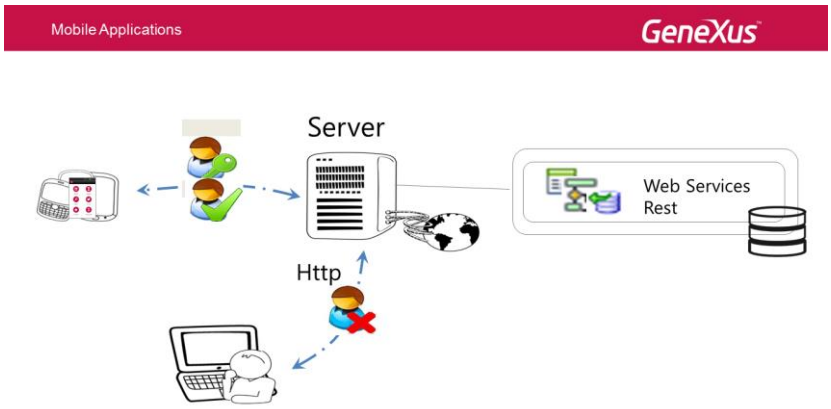
Tradicionalmente se programa un procedimiento que contiene la lógica de control de acceso. Este procedimiento debe verificar los roles y permisos de cada usuario que ingresa a la aplicación.

Cuantos más roles y permisos se tengan y más complejas se hagan las políticas de seguridad de las empresas, el código crece y se hace más complicada la verificación de permisos, que se deben replicar en cada objeto.



En el caso de las aplicaciones para Smart Devices, al ser aplicaciones distribuidas, una parte de ellas se ejecuta en el propio dispositivo y la capa de negocios de la aplicación se resuelve a través de servicios Rest, por lo que están expuestas a accesos indeseados.

Lo que se hace es verificar que solamente usuarios debidamente autenticados y autorizados puedan acceder a la aplicación, evitando la ejecución de usuarios sin los permisos correspondientes.

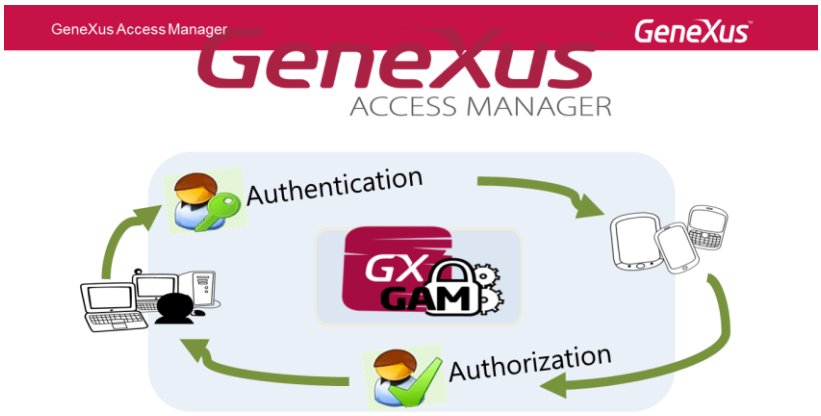


Estos aspectos son los que motivaron el desarrollo de un módulo de Seguridad para aplicaciones GeneXus, llamado GAM, GeneXus Access Manager, y es lo que vamos a utilizar en nuestra aplicación para manejar la Seguridad.

El GAM es un módulo de seguridad que resuelve los problemas de autenticación y autorización, tanto para aplicaciones Web como para aplicaciones Smart Devices con GeneXus.

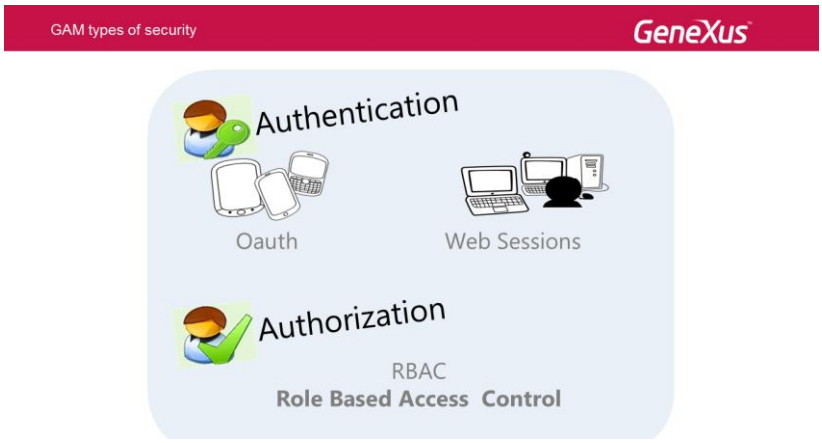
Con el GAM, lo que se busca es que la solución de Seguridad se utilice lo más declarativamente posible dentro de la aplicación, sin crear complejidad en el código.

Esto se puede lograr fácilmente, ya que el GAM es un Módulo de Seguridad desarrollado en una **KB GX**, que se integra a nuestra aplicación y permite resolver de manera centralizada todo lo referente a la Seguridad de la misma.

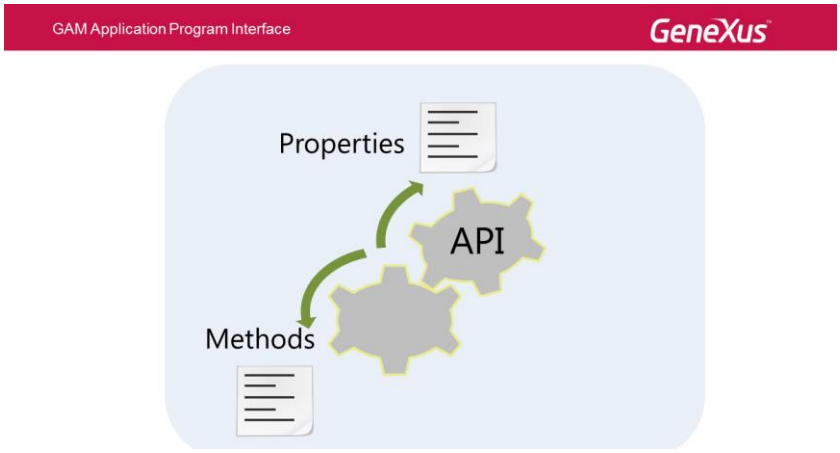


Internamente para resolver la Autenticación, se usa Oauth para el caso de las aplicaciones para Smart Devices y Web Sessions para resolver la seguridad de las aplicaciones WEB.

En el caso de la Autorización, está basada en Roles, utilizando el modelo Role Based Access Control, mediante el cual se encapsulan los métodos, propiedades y todo lo necesario para el manejo de la autorización, para acceder a diferentes partes de la aplicación.

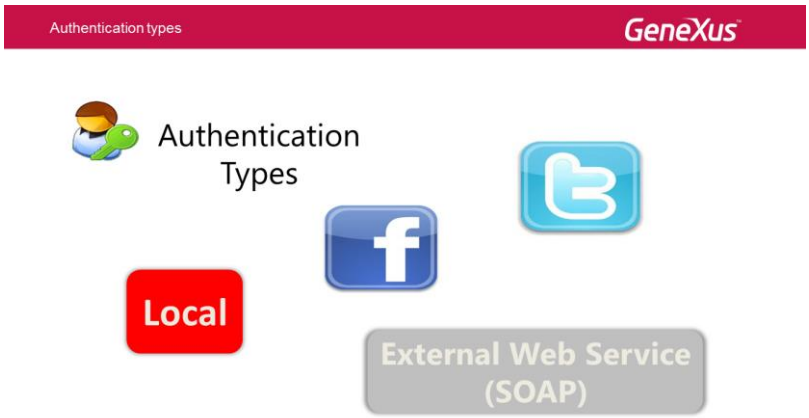


Además el GAM expone una API para acceder a sus métodos y propiedades, en caso de que sea necesario hacerlo desde nuestra aplicación.



Con respecto al proceso de Autenticación, el GAM nos provee diferentes mecanismos:

- **Autenticación local,** donde los usuarios y todas sus credenciales son almacenados en una base de datos de la cual somos propietarios
- **Facebook y Twitter, a**quí se utilizan los mecanismos de autenticación de estas aplicaciones, no teniéndose que definir usuarios locales. La autenticación se realiza en el sitio de FB o Twitter respectivamente
- Se puede también autenticar contra **servicios Web externos**, usando el repositorio de usuarios y roles de otra aplicación, facilitando de esta forma la integración de aplicaciones



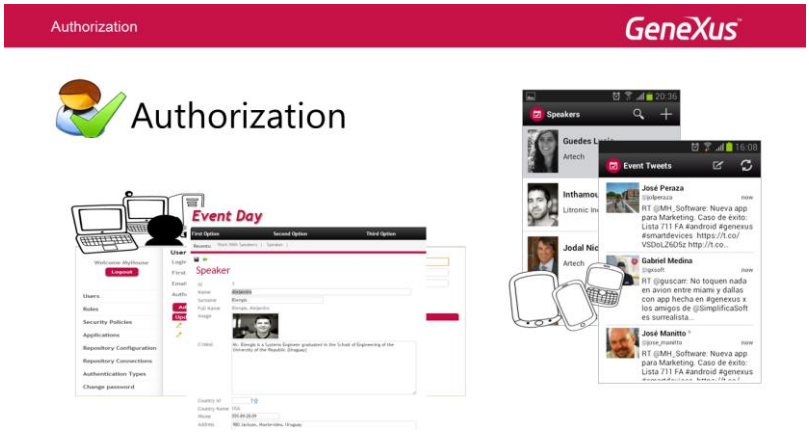
En cuanto a la Autorización, se valida la Autorización de ejecución de objetos.

En caso de objetos web, esta validación se realiza sobre:

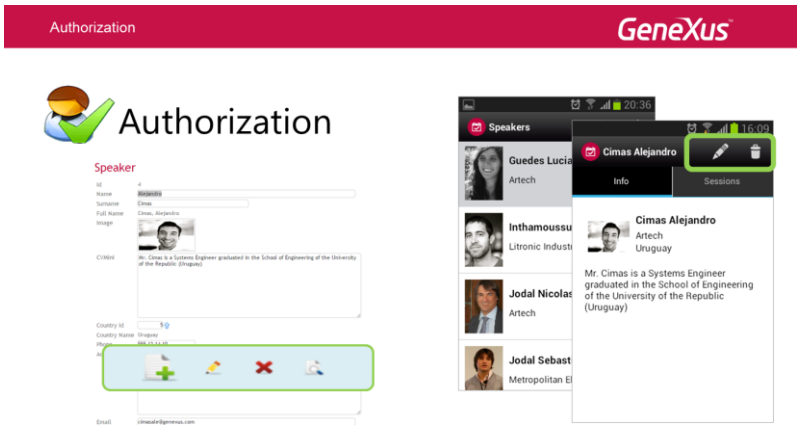
- Web Panels
- Web Components con la propiedad URL Access=Yes y
- Transacciones Web

En el caso de Smart Devices, sobre:

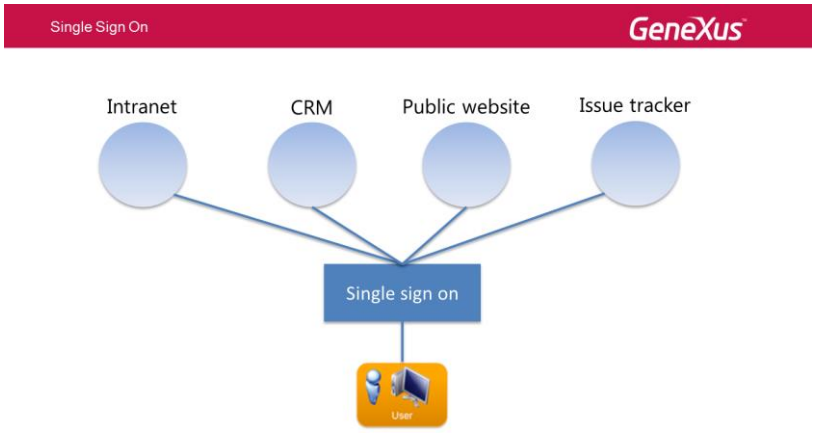
- Work With for Smart Devices y
- Panels for Smart Devices



También se verifican los permisos sobre los modos Insert, Update, Delete y Display de las Transacciones Web y las acciones de Insert, Update y Delete sobre los Work With for Smart Devices.



Otra funcionalidad interesante que nos provee el GAM es la facilidad de loguearnos una única vez y que esas credenciales sirvan para validar el acceso a múltiples aplicaciones.



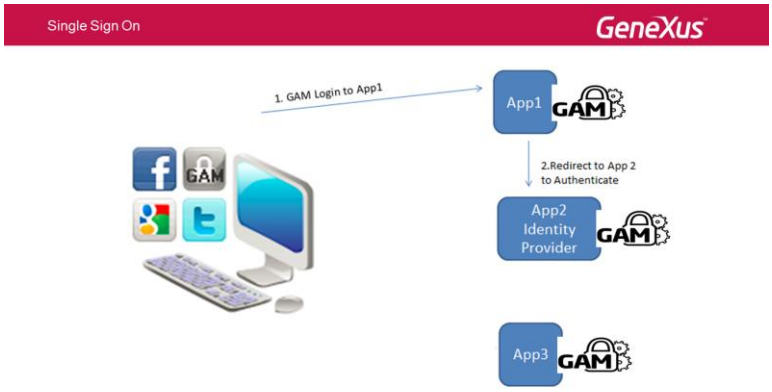
Esta forma de loguearse se denomina “Logueo único” o “Single Sign-in” en su término en inglés.

Esta funcionalidad resuelve el problema de proporcionar autenticación centralizada para diferentes aplicaciones web distribuídas.
En el caso de dos o más aplicaciones Web GeneXus, el usuario sólo tendrá que autenticarse una vez, cuando la primera aplicación que requiere autenticación, pida el usuario para iniciar sesión.
Una vez que la sesión se valida, el usuario no tendrá que introducir sus credenciales de nuevo, incluso después de cambiar a otra aplicación web. La autenticación será válida para todas las aplicaciones Web.

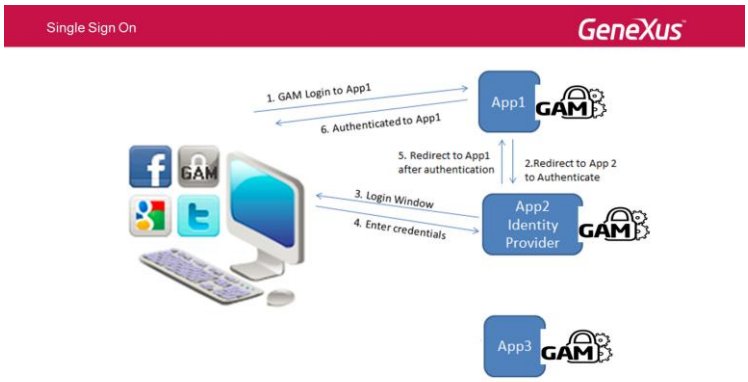
En este escenario, todas las aplicaciones web que participan necesitan utilizar GAM, y uno de ellos se debe configurar como el Proveedor de Identidad.

GAM, que es el proveedor de identidad, se utilizará para autenticar las otras aplicaciones (lo mismo que sucede con Facebook, Twitter y Google, todos los cuales son proveedores de identidad). Consideremos un escenario con tres aplicaciones web: App1, App2 y App3, donde App2 es la aplicación del proveedor de identidades.

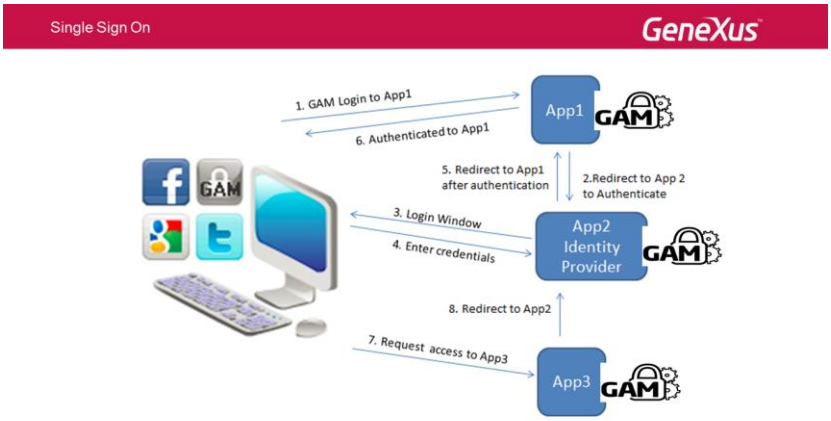
Al comienzo, el usuario intenta ejecutar un objeto privado de App1, y éste lo redirige a la aplicación del proveedor de identidad App2.



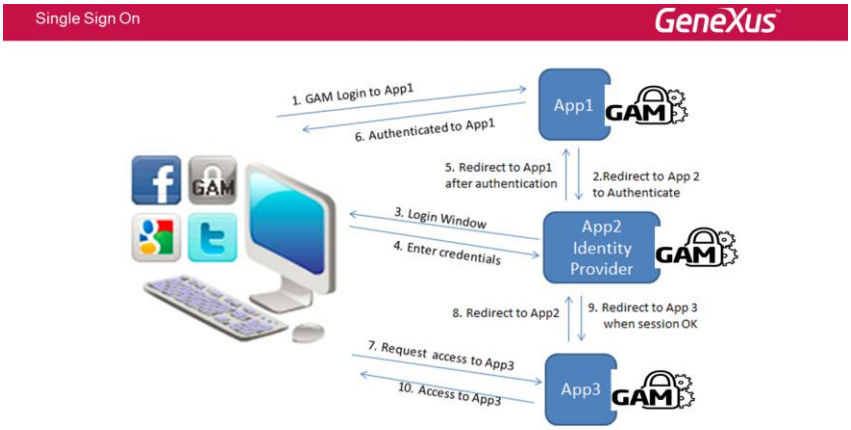
Luego se muestra al usuario el inicio de sesión, el mismo se identifica y después hay una redirección automática a App1.



Tras iniciar sesión en App1, si el usuario intenta ejecutar un objeto privado de App3 desde el mismo navegador web, éste vuelve a dirigirlo al proveedor de identidad App2.

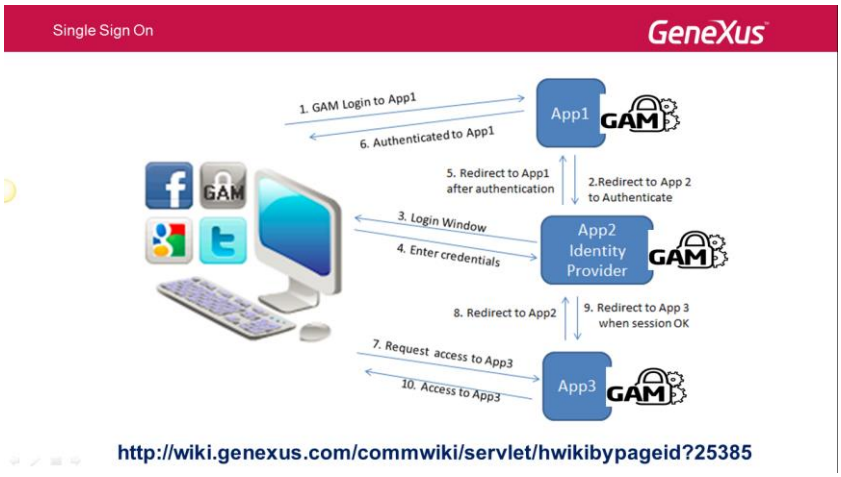


Si el login es válido (ya hay una sesión válida para ese usuario), el inicio de sesión no se muestra al usuario final, y tiene acceso a App3.



Vemos que esto es muy similar a lo que ocurre con Facebook y Twitter; cuando el usuario inicia sesión en cualquiera de estos sitios, las aplicaciones que los utilizan como proveedores de identidad usan la misma sesión válida, si se ejecutan en la misma ventana del navegador.

Para ver cómo configurar las propiedades del GAM para implementar esta funcionalidad, vaya a la dirección que se muestra en pantalla.



En el próximo video de este tema, veremos cómo configurar las propiedades en GeneXus para agregar la seguridad del módulo GAM a nuestra aplicación.