Introducción GAM

Nuestro problema a resolver será construir una aplicación para una inmobiliaria, con una parte Web y una parte para Smart Devices para ser utilizada por los agentes inmobiliarios en su trabajo móvil.

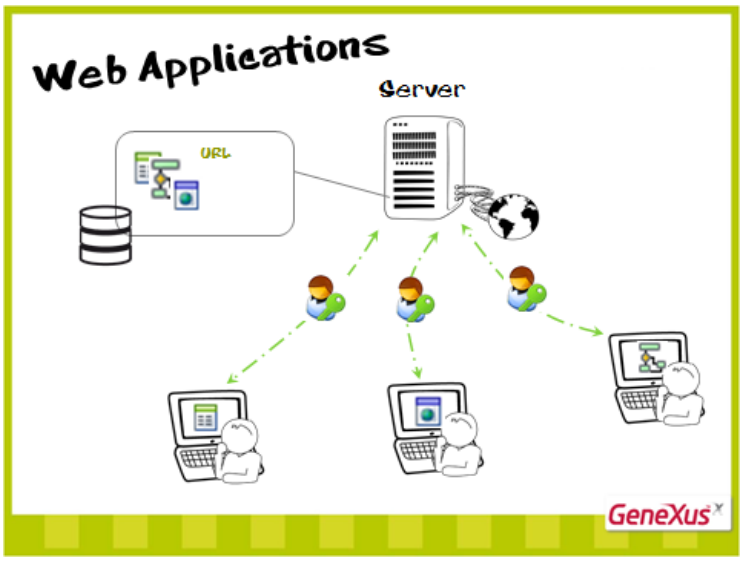
Para ello creamos una KB, y las transacciones necesarias: Property para registrar las propiedades inmobiliarias en venta o alquiler y Neighborhood para ingresar los vecindarios donde están ubicadas las propiedades.

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).

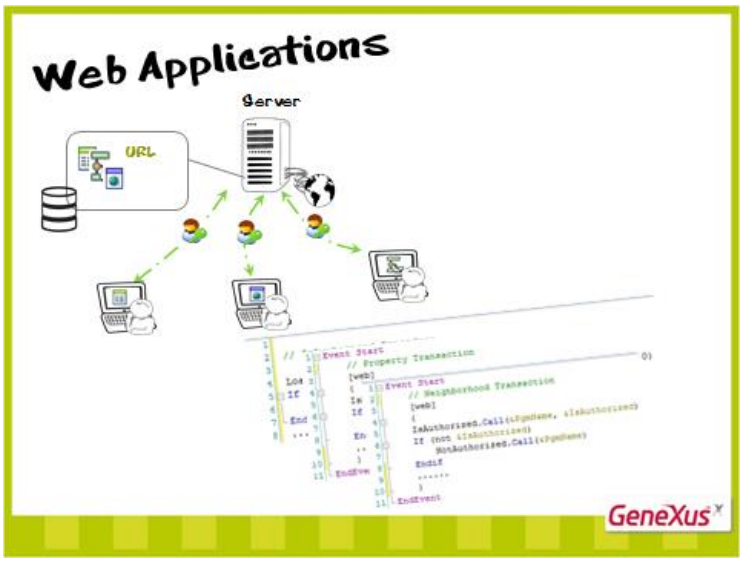
Veamos qué debe tener en cuenta el desarrollador GeneXuys paraa implementar una solución al problema de la seguridad de las aplicaciones.

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



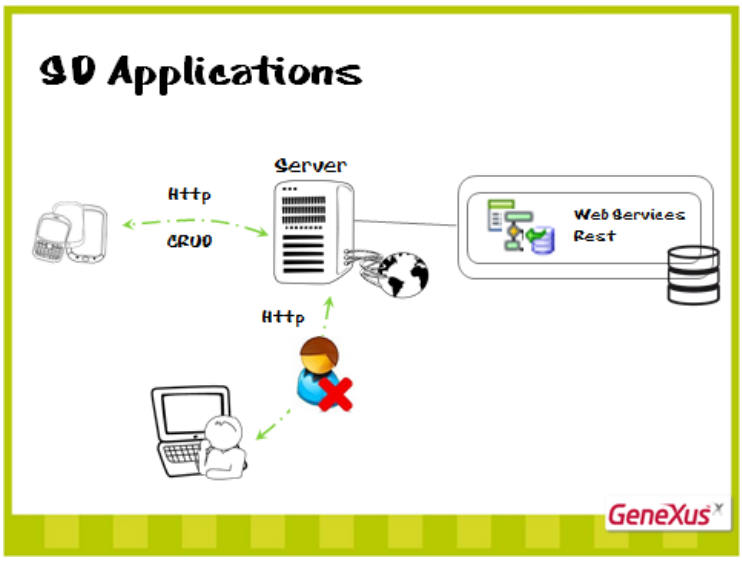
Tradicionalmente se programa un procedimiento que contiene la lógica de control de acceso, este procedimiento debe verificar los roles y permisos de cada usuario que ingresa a la aplicación.

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



En el caso de las aplicaciones para Smart Devices, al ser aplicaciones distribuidas, donde una parte de ellas ejecuta en el propio dispositivo y la capa de negocios de la aplicación se resuelve a través de servicios Rest, 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 no autorizados.

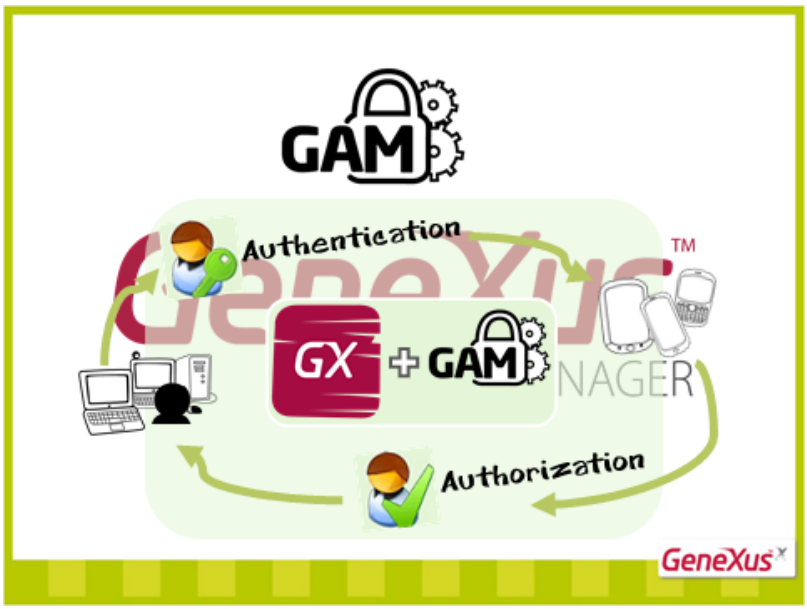


Estos aspectos son los que motivaron el desarrollo de un módulo de Seguridad para aplicaciones GeneXus, llamado GAM, GeneXus Access Manager, y es lo que vamos a utilizar en nuestra aplicación para manejar la Seguridad.

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.

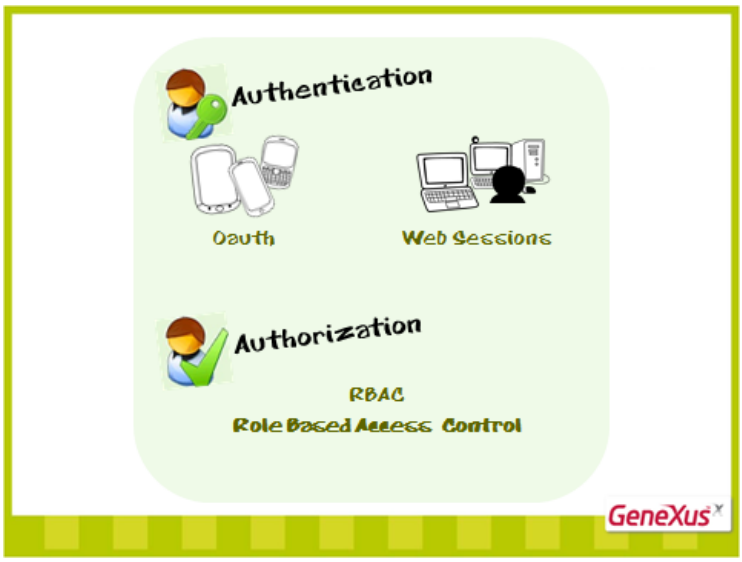
Con el GAM lo que se busca es que la solución de Seguridad se utilice lo más declarativamente posible dentro de la aplicación, sin crear complejidad en el código.

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.

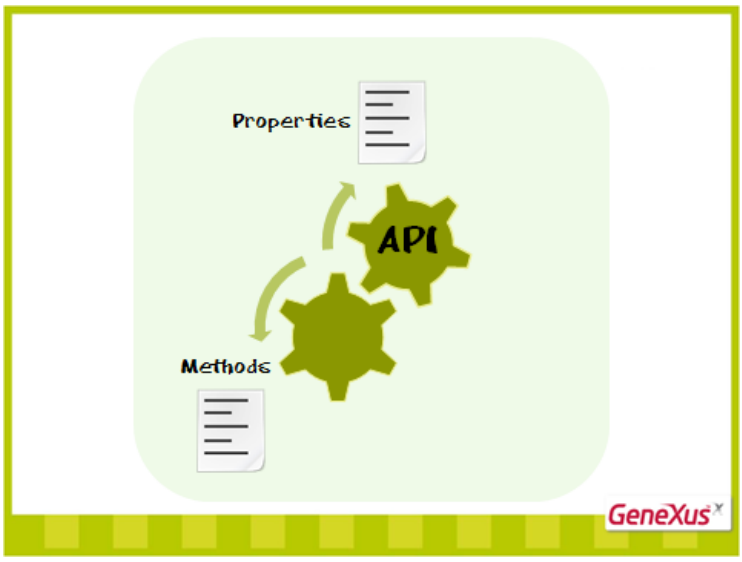


Internamente para resolver la Autenticación, se usa Oauth para el caso de las aplicaciones para Smart Devices y web sessions para resolver la seguridad de las aplicaciones WEB.

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

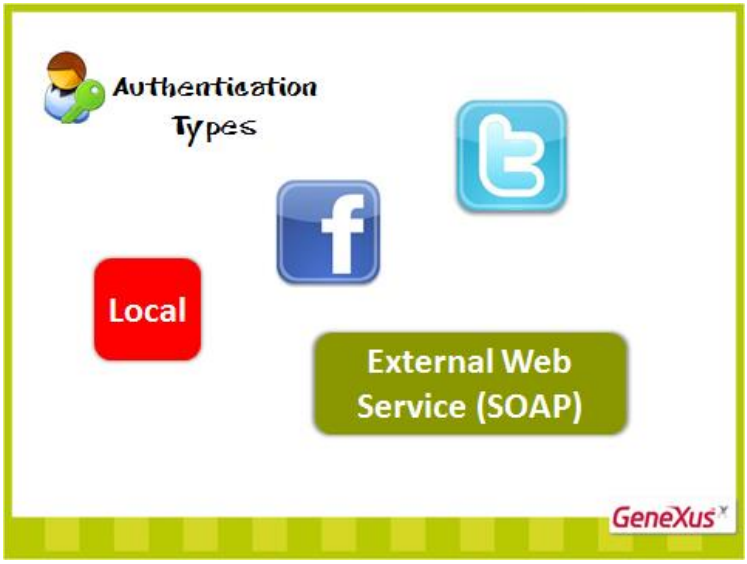


Además el GAM expone una API para acceder a estos métodos y propiedades en caso de que sea necesario hacerlo desde nuestra aplicación.



El GAM provee diferentes Tipos de Autenticación:

- **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, o sea si se pueden ejecutar o no.

Esta validación se realiza sobre:

- Web Panels
- Web Components con la propiedad URL Access=Yes
- 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.