# Introdução: GAM


O problema a ser resolvido é construir um aplicativo para uma imobiliária, com uma parte para Internet e outra para Smart Devices, a ser utilizado pelos corretores em seu trabalho móvel.

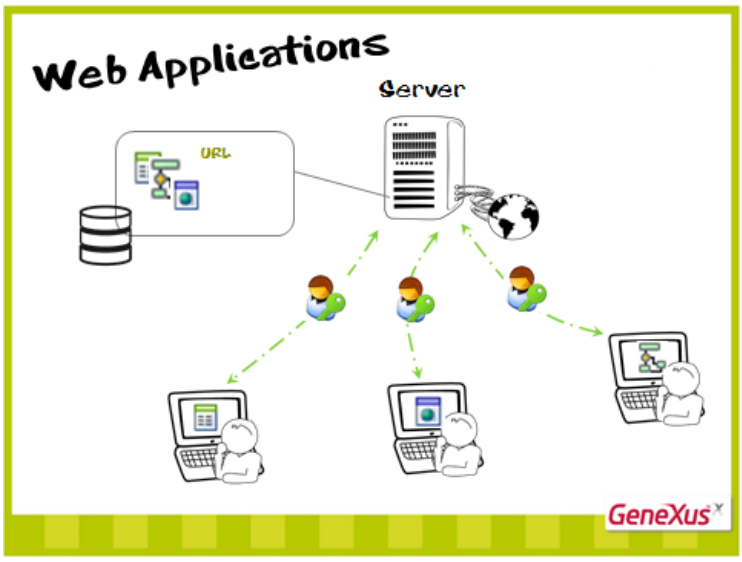
Para isso, criamos uma KB, Knowledge Base, e as transações necessárias: Property, para registrar os imóveis à venda ou locação e Neighborhood, para entrar nas vizinhanças onde estão localizados os imóveis.

O que se pretende, agora, é acrescentar Segurança ao aplicativo, tanto na parte para Internet como para Smart Devices.


Isso significa assegurar que todos os usuários, ao ingressarem, estejam devidamente autenticados (que o usuário seja quem diz ser) e autorizados (uma vez que o usuário se autentica, seja ou não permitido seu acesso a certas partes do aplicativo).

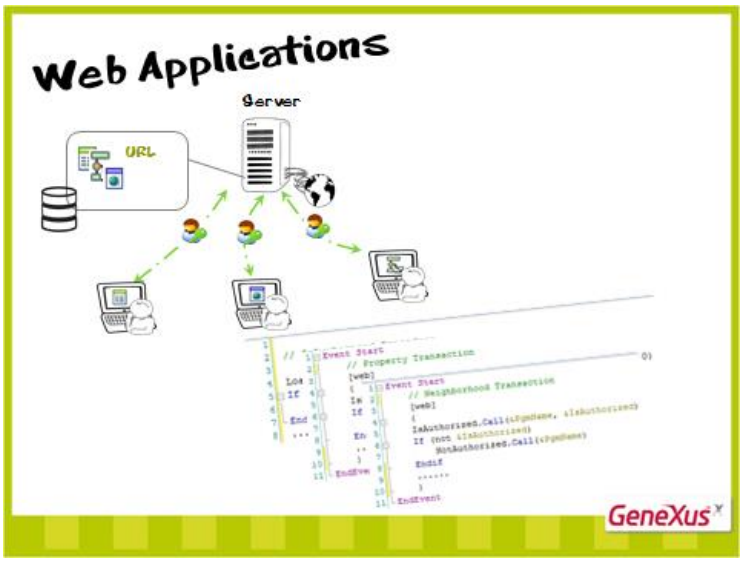

Veja o que deve considerar o desenvolvedor GeneXus para implementar uma solução ao problema da segurança dos aplicativos.

No caso dos aplicativos para Internet, como há vários pontos de entrada, deve-se checar as permissões de autenticação de qualquer objeto acessível por URL.



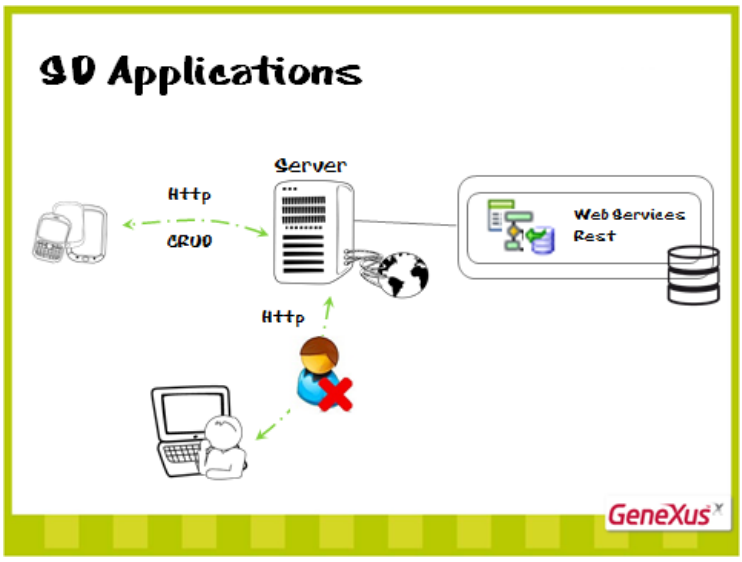

Tradicionalmente, programa-se um procedimento que contém a lógica do controle de acesso, tal procedimento deve verificar as funções e permissões de cada usuário que entra no aplicativo.

Quanto mais funções e permissões se têm e mais complexas são as políticas de seguranças das empresas, mais o código cresce e mais complicada se torna a verificação de permissões, que se deve replicar em cada objeto e evento.




Os aplicativos para Smart Devices, por serem aplicativos distribuídos, em que uma parte deles executa no próprio aparelho e o grupo de negócios do aplicativo se resolve através dos serviços REST, estão expostos a acessos indesejados.

O que se faz é garantir que somente os usuários devidamente autenticados e autorizados possam entrar no aplicativo, evitando que usuários não autorizados o executem.

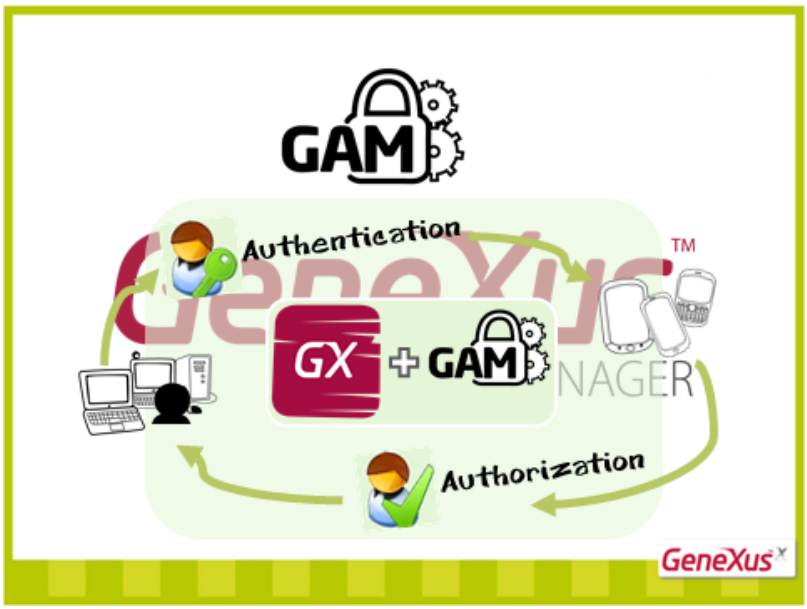



Esses aspectos são os que motivaram o desenvolvimento de um módulo de segurança para aplicativos GeneXus, chamado GAM, GeneXus Access Manager, que se utilizará no aplicativo para tratar da segurança.


O GAM é um módulo de segurança que resolve os problemas de autenticação e autorização, tanto para aplicativos para Internet como para aplicativos para Smart Devices com GeneXus.

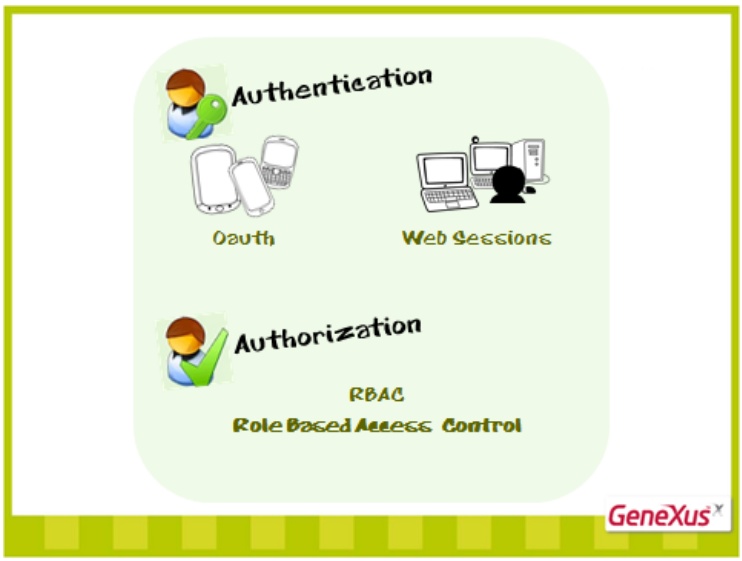
O que se busca com o GAM é que a solução de Segurança seja o mais declarativamente possível dentro o aplicativo, sem tornar código complexo.

Pode-se conseguir isso facilmente, já que o GAM é um módulo de Segurança desenvolvido em uma **KB GX**, que se integra ao aplicativo e permite resolver de maneira centralizada tudo o que se refere a sua Segurança.

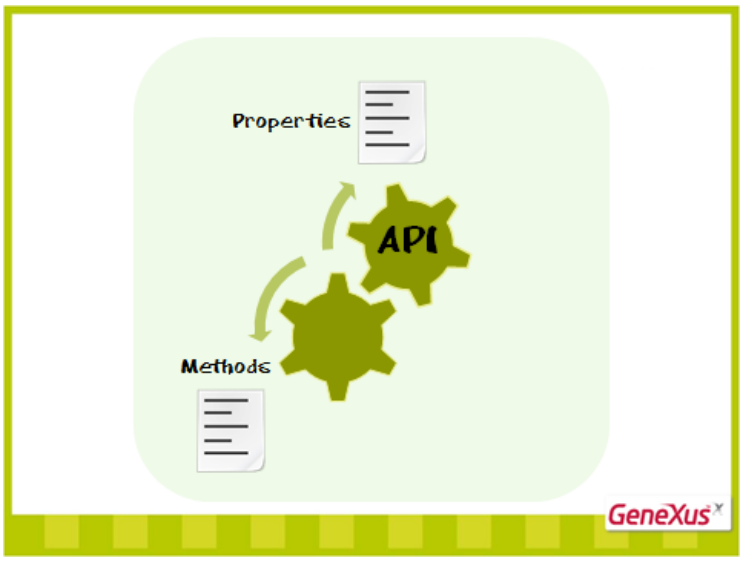



Internamente, para resolver a Autenticação, usa-se o Oauth para o caso dos aplicativos para Smart Devices, e Web Sessions para resolver a segurança dos aplicativos para Internet.

A Autorização está baseada em funções, utilizado o modelo RABC, Role Based Access Control. Encapsulam-se os métodos, as propriedades e tudo que é necessário para o desenvolvimento da autorização no aplicativo.

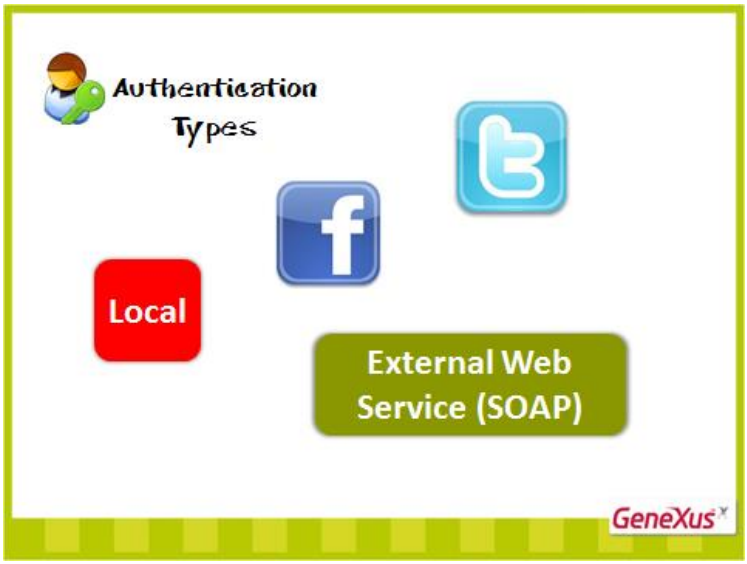



Além disso, o GAM expõe uma API para ter acesso a esses métodos e propriedades, caso seja necessário fazê-lo a partir de nosso aplicativo.




O GAM fornece diferentes Tipos de Autenticação:

- **Autenticação Local**, em que os usuários e todas suas informações são armazenados em uma base de dados da qual somos proprietários;
- **Facebook** e **Twitter**, utilizam-se os mecanismos de autenticação destes aplicativos e não é preciso definir os usuários locais. A autenticação se realiza nos sites do FB ou Twitter, respectivamente;
- Pode-se também autenticar contra os **serviços Web externos**, utilizando o registro de usuários e funções de outro aplicativo; facilitando, assim, a integração de aplicativos.



Quanto à Autorização, valida-se a Autorização de execução de objetos, isto é, define-se se é ou não possível a execução.

Esta validação realiza-se sobre:

- Web Panels
- Web Components com a propriedade URL Access = Yes
- Transações Web

Nos casos de Smart Devices, sobre Work With for Smart Devices e Panels for Smart Devices


Também se verificam as permissões sobre os modos Insert, Update, Delete e Display das transações para Internet e as ações de Insert, Update e Delete sobre os Work With for Smart Devices.