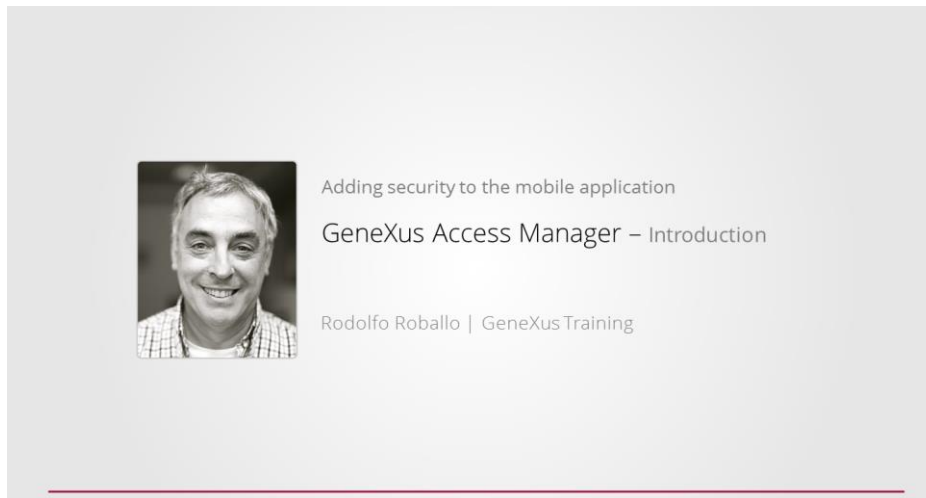


Introdução ao GAM



Nos vídeos anteriores vimos o desenvolvimento de uma aplicação web e para dispositivos móveis, para administrar os dados de um evento, com informação de suas conferências, oradores, etc.

Introduction

Event Day

First Option

Recently | Home | Work With Speakers |

Work With Speakers

Name

	ID	Name	Surname	Full Name	Image	CVMini	Country Id	Country Name
	7	Alejandro	Biangio	Biangio, Alejandro		Mr. Biangio is a Systems Engineer graduated in the School of Engineering of the University of the Republic (Uruguay)	1	USA
	4	Alejandro	Cimas	Cimas, Alejandro		Mr. Cimas is a Systems Engineer graduated in the School of Engineering of the University of the Republic (Uruguay)	5	Usoabate
	12	Armando	Cardozo	Cardozo, Armando		Mr. Cardozo is a Systems Engineer graduated in the School of Engineering of the University of the Republic	5	Usoabate

Agora queremos aumentar a Segurança da aplicação, tanto na parte web como a de Smart Device.



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

Security
GeneXus™

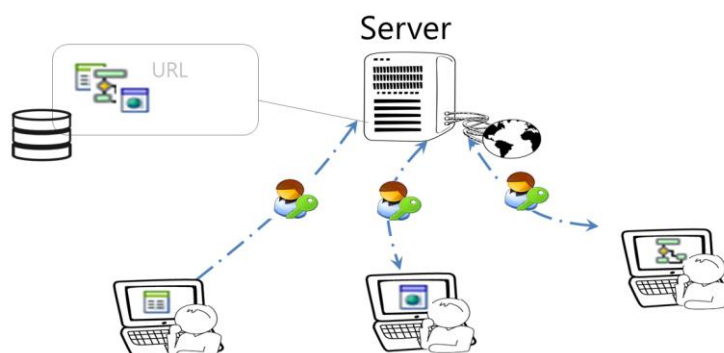
Authentication

Authorization

Select	Permission name	Description	Access type
☒	property_Delete	Property Delete	Allow
☒	property_Execute	Property	Allow
☒	property_FullControl	Property FullControl	Allow
☒	property_Insert	Property Insert	Allow
☐	property_Services_Delete	Property Services Delete	Allow
☐	property_Services_Execute	Property Services	Allow
☐	property_Services_FullControl	Property Services FullControl	Allow
☐	property_Services_Insert	Property Services Insert	Allow
☐	property_Services_Update	Property Services Update	Allow

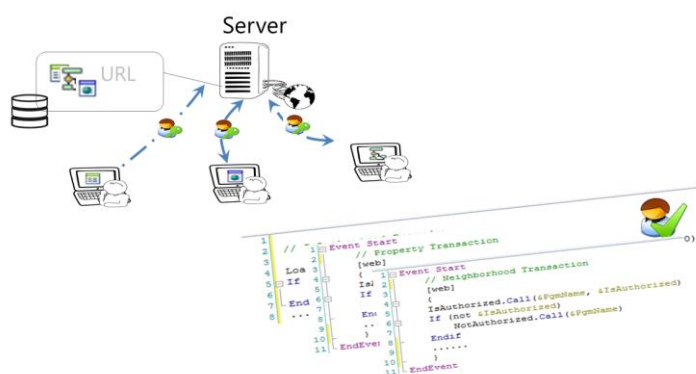
Vejamos o que deve considerar o desenvolvedor Genexus para implementar uma solução para o problema da segurança das aplicações.

No caso das aplicações Web, como há vários pontos de entrada, deve-se checar as permissões de autenticação de qualquer objeto acessível por URL.



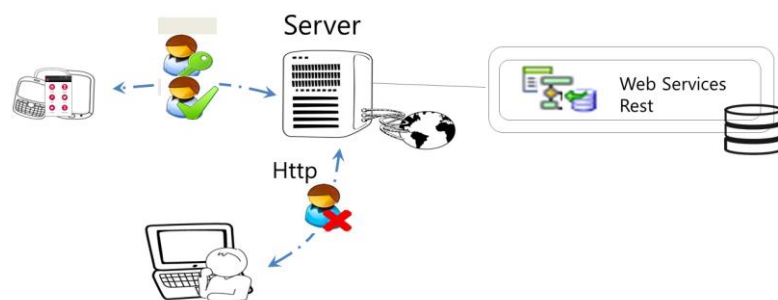
Tradicionalmente programa-se um procedimento que contém a lógica de controle de acesso. Este procedimento deve verificar as funções e permissões de cada usuário que entrar na aplicação.

Quanto mais funções e permissões tiver, mais complexa será a política de segurança das empresas, mais o código cresce e mais complicado se torna a verificação de permissões, que deve ser replicada em cada objeto.



No caso das aplicações para Smart Devices, por ser aplicativos distribuídos, em que uma parte delas se executa no próprio dispositivo e a camada de negócios da aplicação é resolvido através dos serviços Rest, onde estão expostos a acessos indesejados.

O que deve fazer é garantir que somente usuários devidamente autenticados e autorizados possam acessar a aplicação, evitando que usuários sem permissão o executem.



Estes aspectos são os que motivaram o desenvolvimento de um módulo de Segurança para aplicativos GeneXus, chamado GAM, GeneXus Access Manager, que iremos utilizar em nossa aplicação para tratar da Segurança.



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

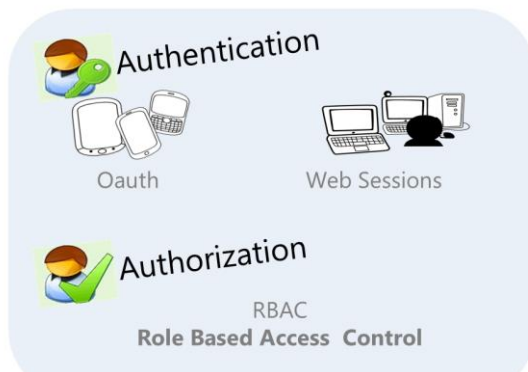
O que se busca com o GAM, é uma solução de Segurança que seja o mais declarativamente possível dentro da aplicação, sem tornar o código complexo.

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

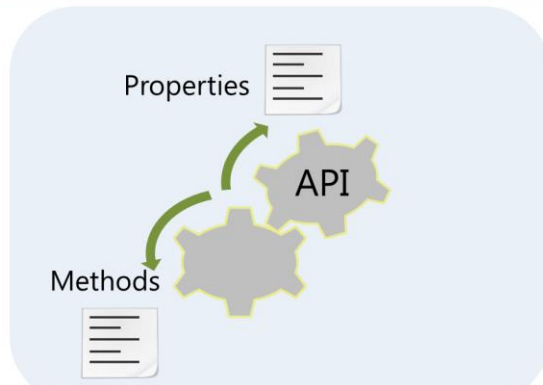


Internamente, para resolver a Autenticação, utiliza-se o Oauth para o caso dos aplicativos para Smart Devices e Web Sessions para resolver a segurança das aplicações WEB.

No caso da Autorização, está baseada em funções, utilizando o modelo Role Based Access Control, mediante o qual são encapsulados os métodos, as propriedades e tudo o que for necessário para o desenvolvimento da autorização na aplicação, para acessar as diferentes partes da aplicação.

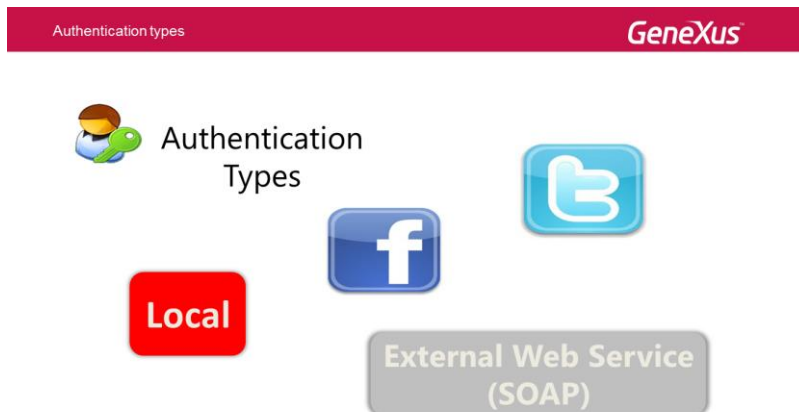


Além disso, o GAM expõe uma API para ter acesso a esses métodos e propriedades, caso seja necessário fazê-lo a partir de nossa aplicação.



A respeito do processo de Autenticação, o GAM fornece diferentes mecanismos:

- **Autenticação local**, onde os usuários e todas suas credenciais são armazenadas numa base de dados da qual somos proprietários.
- **Facebook e Twitter**, utilizam-se os mecanismos de autenticação destas aplicações, e não é preciso definir os usuários locais. A autenticação é realizada nos sites do FB ou Twitter, respectivamente.
- Pode-se também autenticar contra os **serviços Web externos**, utilizando o registro de usuários e funções de outra aplicação, facilitando desta forma a integração de aplicações.



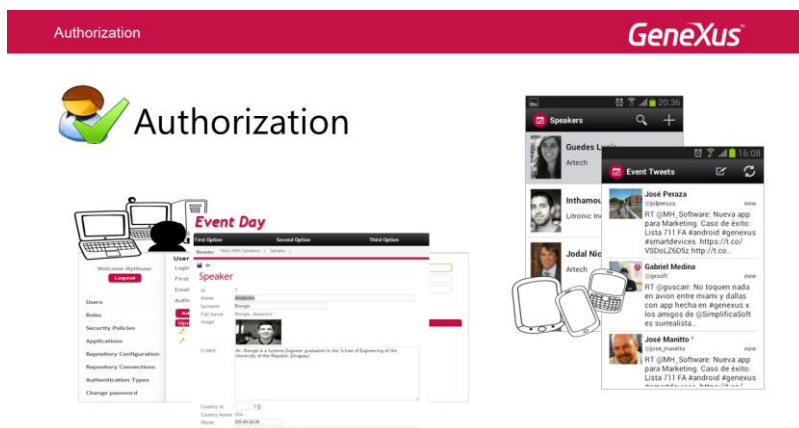
Quanto à Autorização, valida-se a autorização da execução de objetos.

No caso de objetos web, esta validação é realizada sobre:

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

No caso de Smart Devices, sobre:

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



Também verificam-se as permissões sobre os modos Insert, Update, Delete e Display das Transações Web e as ações de Insert, Update e Delete sobre os Work With for Smart Devices.



Authorization

Speaker

id:

name:

surname:

full name:

image:

CI0002

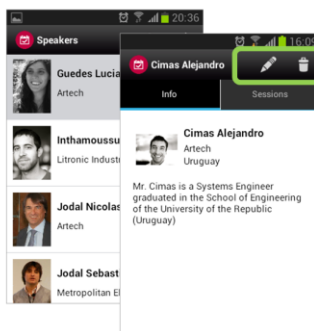
Mr. Cimas is a Systems Engineer graduated in the School of Engineering of the University of the Republic (Uruguay)

Country ID:

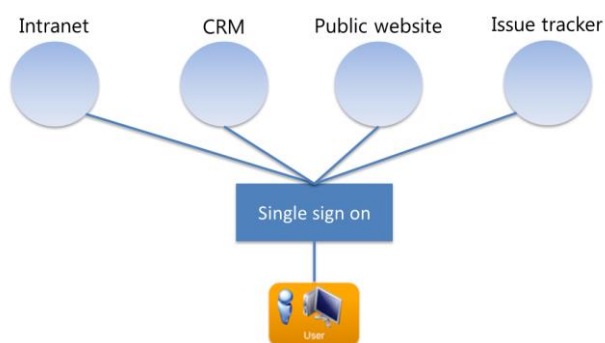
Country Name:

Phone:

Email:



Outra funcionalidade interessante que nos fornece o GAM é a facilidade de logarmos uma única vez e que essas credenciais servem para validar o acesso a múltiplas aplicações.



Esta forma de logar denomina-se “Logue único” ou “Single Sign-on” em inglês.

Esta funcionalidade resolve o problema de proporcionar a autenticação centralizada para diferentes aplicações web distribuídas.

No caso de duas ou mais aplicações Web GeneXus, o usuário somente terá que autenticar-se uma única vez, na primeira aplicação que requer a autenticação, e solicita ao usuário que inicie a sessão.

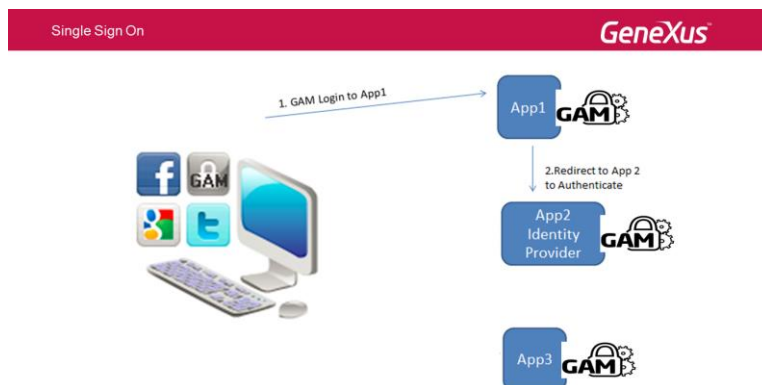
Uma vez que a sessão é validada, o usuário não terá que introduzir suas credenciais novamente, mesmo depois de alterar outra aplicação web. A autenticação é válida para todas as aplicações Web.

Neste cenário, todas as aplicações web que participam necessitarão utilizar o GAM, e um deles deve configurar como o Provedor de Identidade.

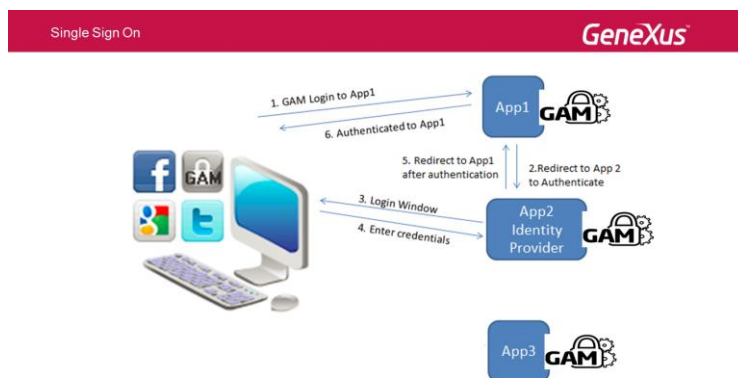


O GAM, que é o provedor de identidade, utilizará para autenticar as outras aplicações (o mesmo que acontece com Facebook, Twitter e Google, todos os quais são provedores de identidade). Consideramos um cenário com três aplicações web: App1, App2 e App3, onde App2 é a aplicação do provedor de identidade.

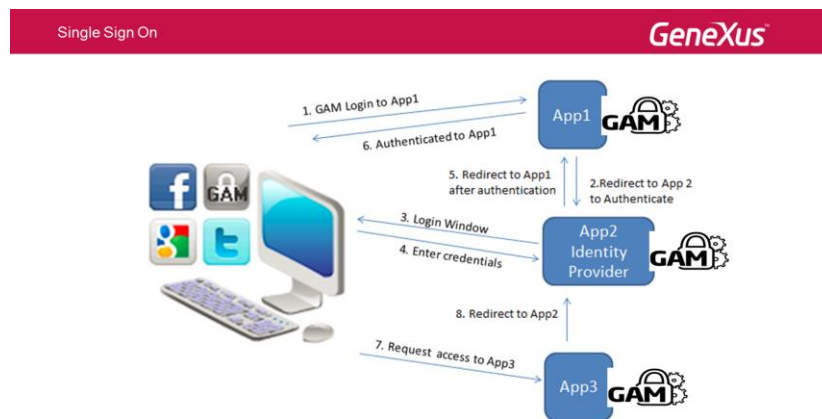
Na primeira, o usuário tenta executar um objeto privado App1, e este redireciona a aplicação do provedor de identidade App2.



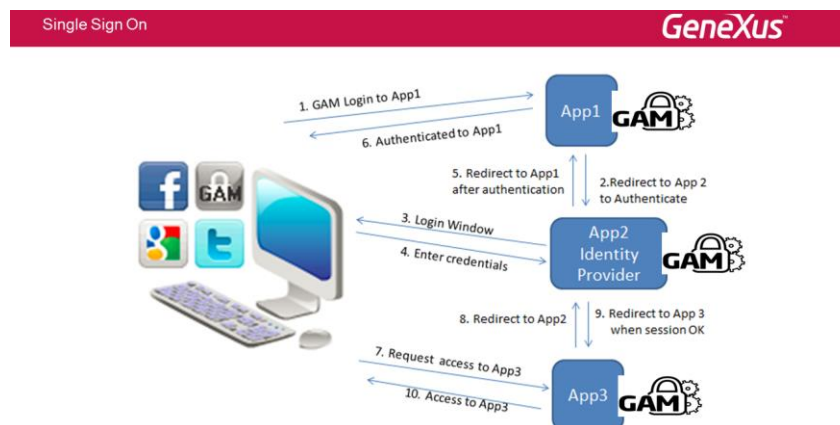
Logo é mostrado ao usuário o início da sessão, o mesmo se identifica e em seguida, há um redirecionamento automático para App1.



Após o iniciar a sessão em App1, se o usuário tentar executar um objeto privado da App3 do mesmo navegador web, este retorna redirecionando ao provedor de identidade App2.

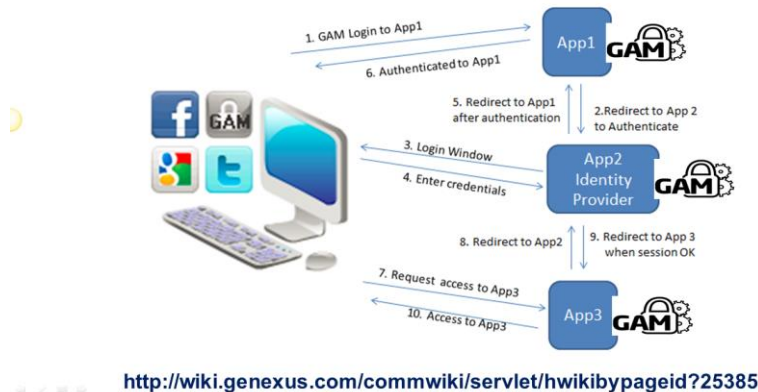


Se o login é válido (já tem uma sessão válida para esse usuário), o início da sessão não é mostrada ao usuário final, e este tem acesso a App3.



Vejamos que isso é muito similar ao que ocorre com o Facebook e Twitter; quando o usuário inicia a sessão em qualquer destes sites, as aplicações que o utilizam como provedores de identidade usam a mesma sessão válida, se executada na mesma janela do navegador.

Para ver como configurar as propriedades do GAM e para implementar esta funcionalidade, vá para o endereço mostrado na tela.



<http://wiki.genexus.com/commwiki/servlet/hwikibypageid?25385>

No próximo vídeo deste tema, veremos como configurar as propriedades no Genexus para aumentar a segurança do módulo GAM na nossa aplicação.