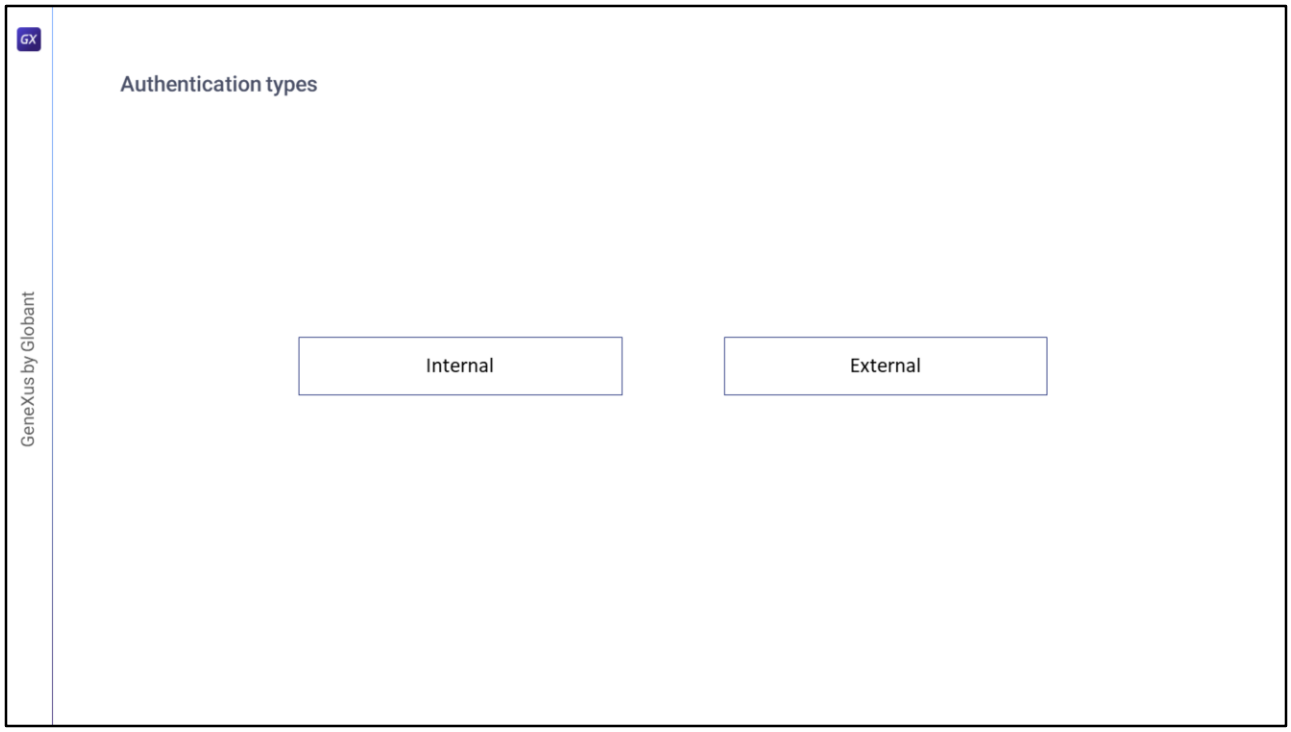

GeneXus by Globant
GeneXus™
by Globant
training.genexus.com

GeneXus by Globant

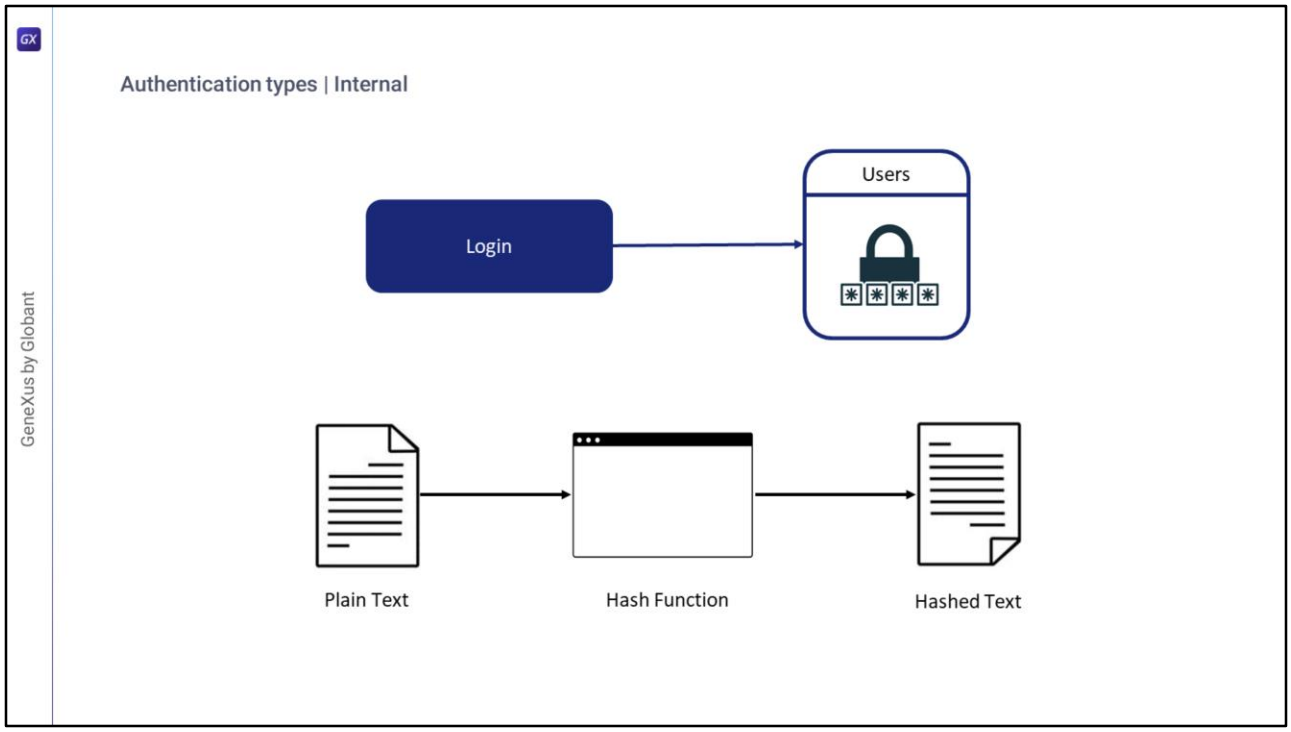
Authentication Types

Nicolas Adrién



Como dissemos em vídeos anteriores, o GAM oferece diferentes tipos de autenticação, tanto internos (contra a base de dados GAM), quanto externos (como serviços web, redes sociais, Google ou também chamados Remotos).

Vamos entrar em detalhes sobre estes.

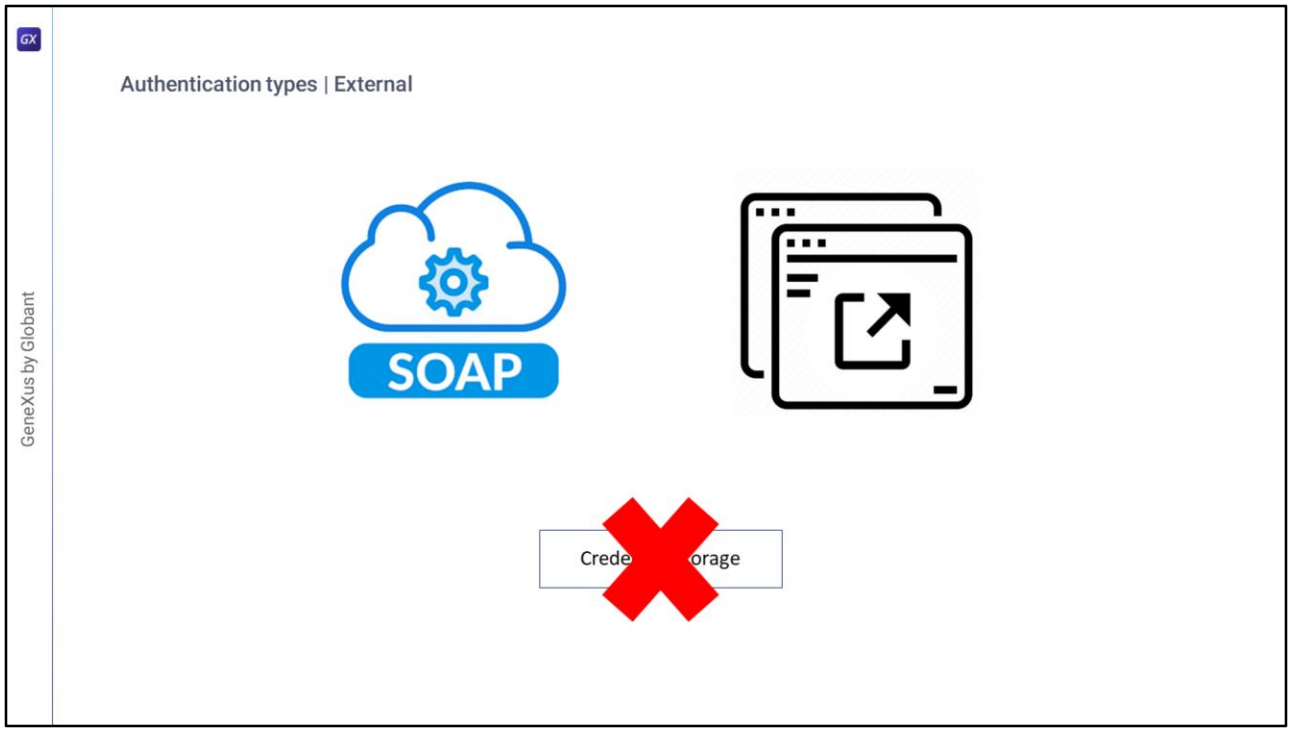


Quanto aos Tipos de Autenticação Internos, temos **Autenticação local**, onde as credenciais dos usuários são armazenadas na tabela "Usuários" do GAM.

GAM não armazena a senha do usuário, mas armazena um hash dela. Um hash é um algoritmo tal que, dada uma string em texto plano, produz sempre a mesma string resultante e, dada esta, não pode ser obtida a original.

O hash é obtido a partir de uma chave única para cada usuário e um algoritmo denominado SHA-512, sobre o qual não entraremos em detalhes.

Isto significa que quando são recuperados Usuários GAM do repositório, a propriedade da senha sempre tem um valor vazio.



Quando é desejado integrar uma aplicação com outra para trocar informação, o primeiro ponto fundamental é resolver o problema da autenticação.

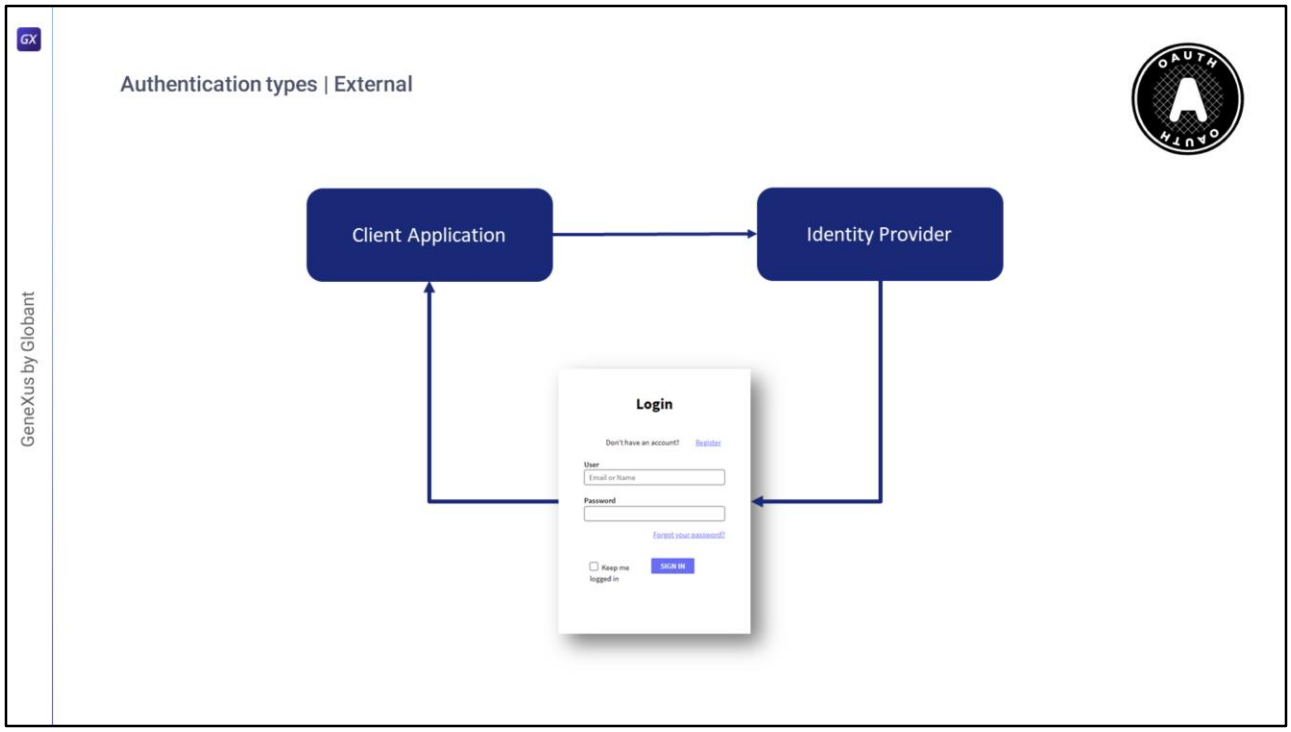
No tipo de autenticação Externo, uma primeira solução é que a aplicação que precisamos integrar exponha um serviço web SOAP que resolva a autenticação.

Outro cenário é o de um programa externo à aplicação que resolve os problemas de autenticação, que não necessariamente é um serviço SOAP. A solução para esse cenário é configurar o tipo de autenticação personalizada de GAM no repositório de GAM.

Em ambos os casos, é necessário configurar GAM para aceitar o programa externo como Identity Provider.

Ao utilizar qualquer um destes tipos de autenticação, o GAM Cliente não é o proprietário das credenciais do usuário, apenas se armazenará no Repositório o nome de usuário e outras informações que dependem da saída do programa externo.

No caso de autenticação em outros serviços externos, como LDAP, pode usar um programa externo ou serviço web para fazer uma ponte entre a aplicação GAM e LDAP.



Entrando no restante de tipos de autenticação, primeiro temos o Oauth 2.0.

GAM permite autenticar-se com qualquer provedor de OAuth na versão 2.0, apenas seguindo algumas etapas simples.

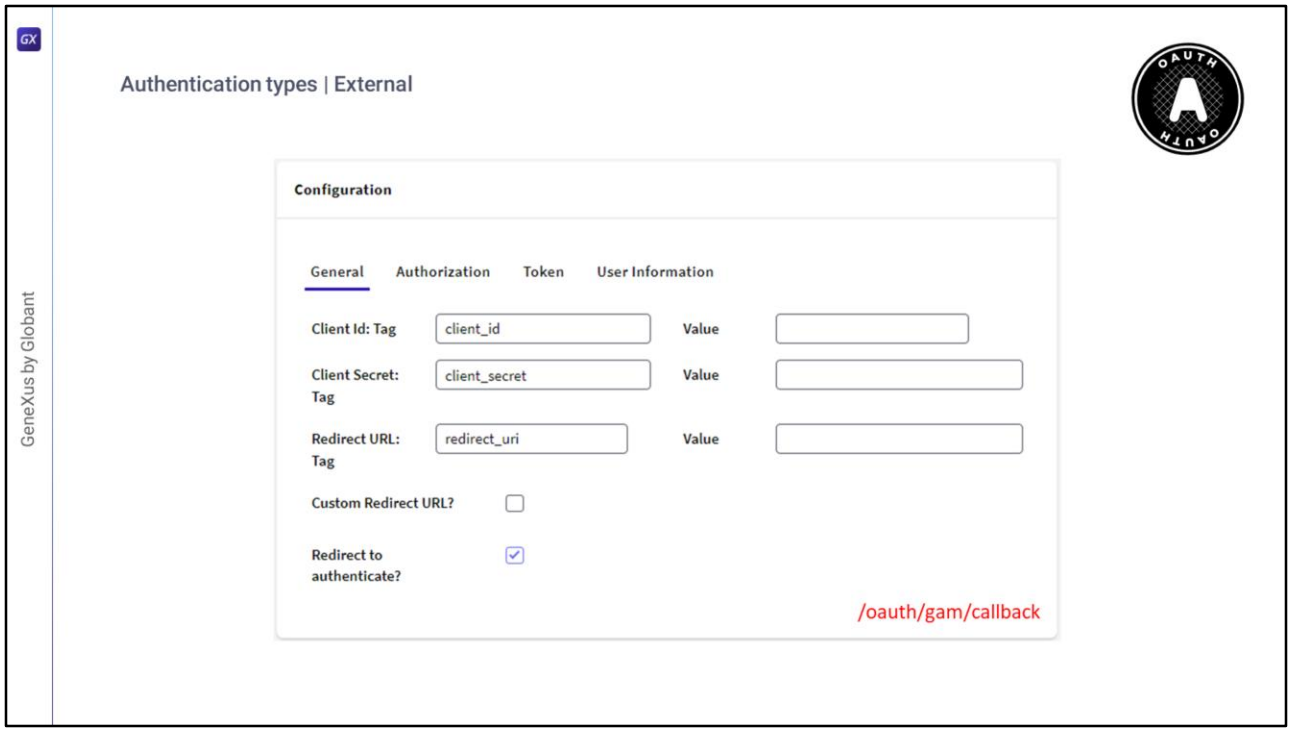
Quando é selecionado este tipo de autenticação, o início de sessão de uma aplicação é redirecionado para o provedor de identidade configurado.

O início de sessão é exibido pelo provedor; e ali os usuários inserem suas credenciais sendo redirecionados novamente para a aplicação.

A definição deste tipo de Autenticação é igual a qualquer um dos outros tipos que já mencionamos de GAM, só que este requer uma configuração detalhada do protocolo utilizado pelo Provedor. Portanto, para configurar o tipo de autenticação OAuth 2.0

no GAM, deve ser seguida a documentação do provedor de identidade ao qual deseja se conectar.

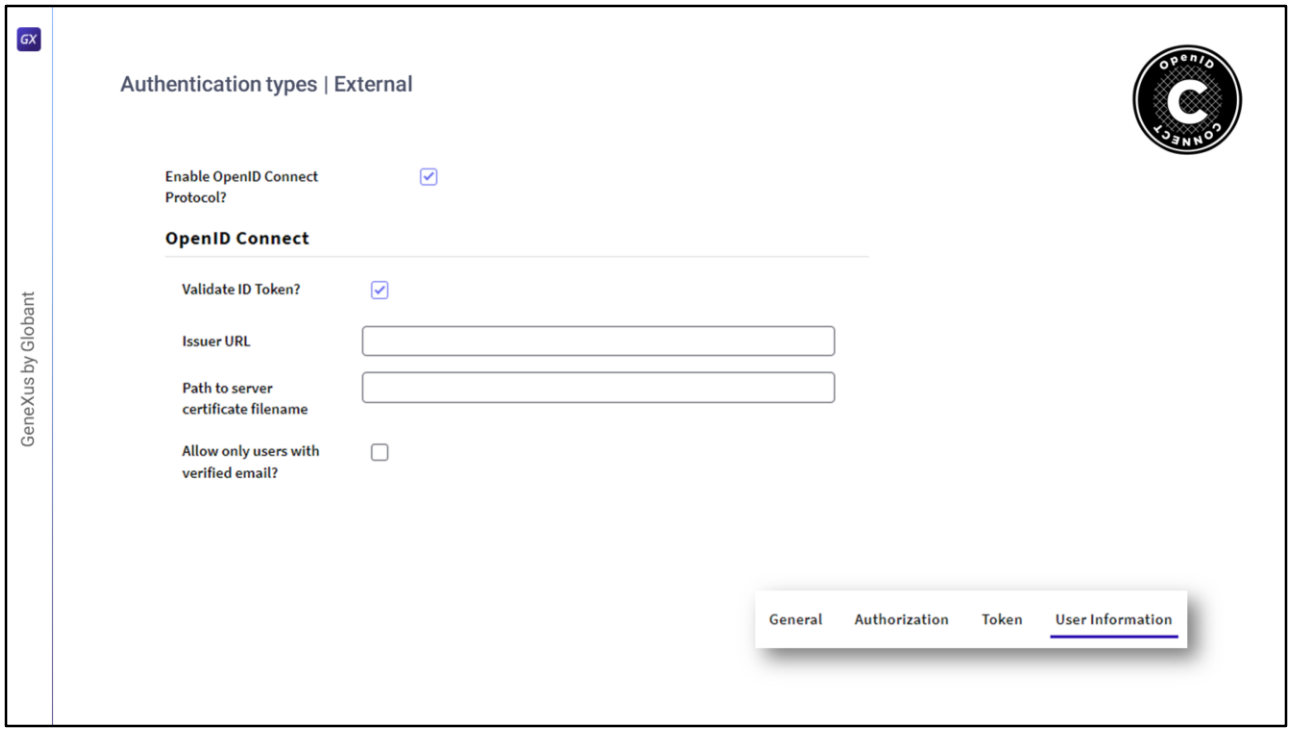
Esse protocolo também resolve o SSO entre diferentes aplicações clientes.



Oauth 2.0 possui um segundo fluxo de autenticação que permite através da opção "Redirecionar para autenticar?" em False a autenticação OAuth 2.0 usando REST sem redirecionar para o provedor de identidade, onde o que faz GAM é pular o redirecionamento configurado na aba Authorization.

A outra opção (Custom Redirect URL?), é onde é especificado para GAM que a URL de retorno indicada é personalizada, a qual se estiver em False, em seguida concatenará "/oauth/gam/callback" como vemos em tela. Por outro lado, se estiver em True, esta URL deve ser implementada pelo desenvolvedor e ler as respostas do IDP.

Ambas as propriedades são configuráveis a partir do tipo de autenticação OAuth a partir do Backend de GAM.



Posteriormente temos OpenID Connect.

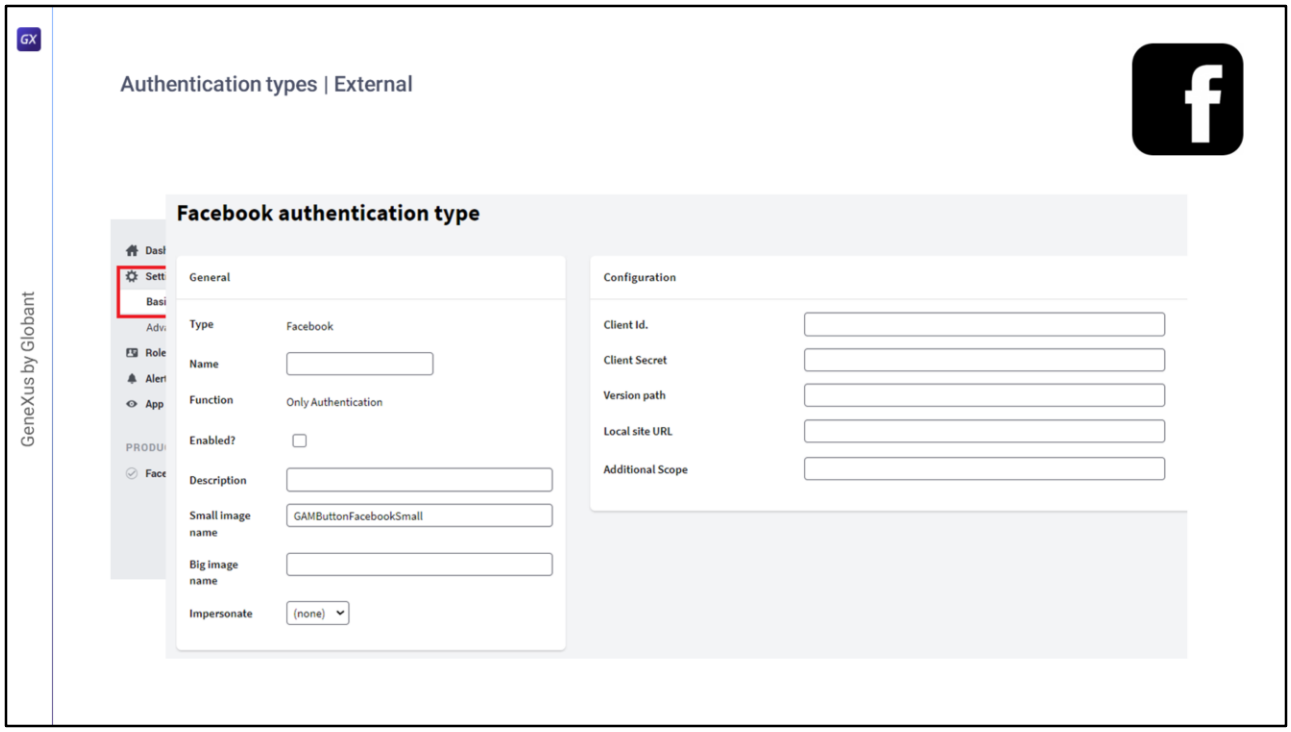
Este é um protocolo de autenticação que funciona com OAuth 2.0 ao implementar a autenticação como uma extensão do processo de autorização de OAuth e está se tornando um dos mais comuns da atualidade.

A vantagem que nos proporciona quanto ao OAuth, é que este protocolo nos permite obter a informação do usuário enquanto no padrão de OAuth não temos como obter essa informação. Por esta razão é que agora não é necessário configurar a seção de

User Information no Authentication Type.

Para que o protocolo funcione, deve ser ativada a propriedade Validate ID Token e incluir quem é o provedor e o certificado público local em um servidor.

Com esta informação, é obtido um JSON Web Token assinado e retornado pelo provedor, denominado ID Token.

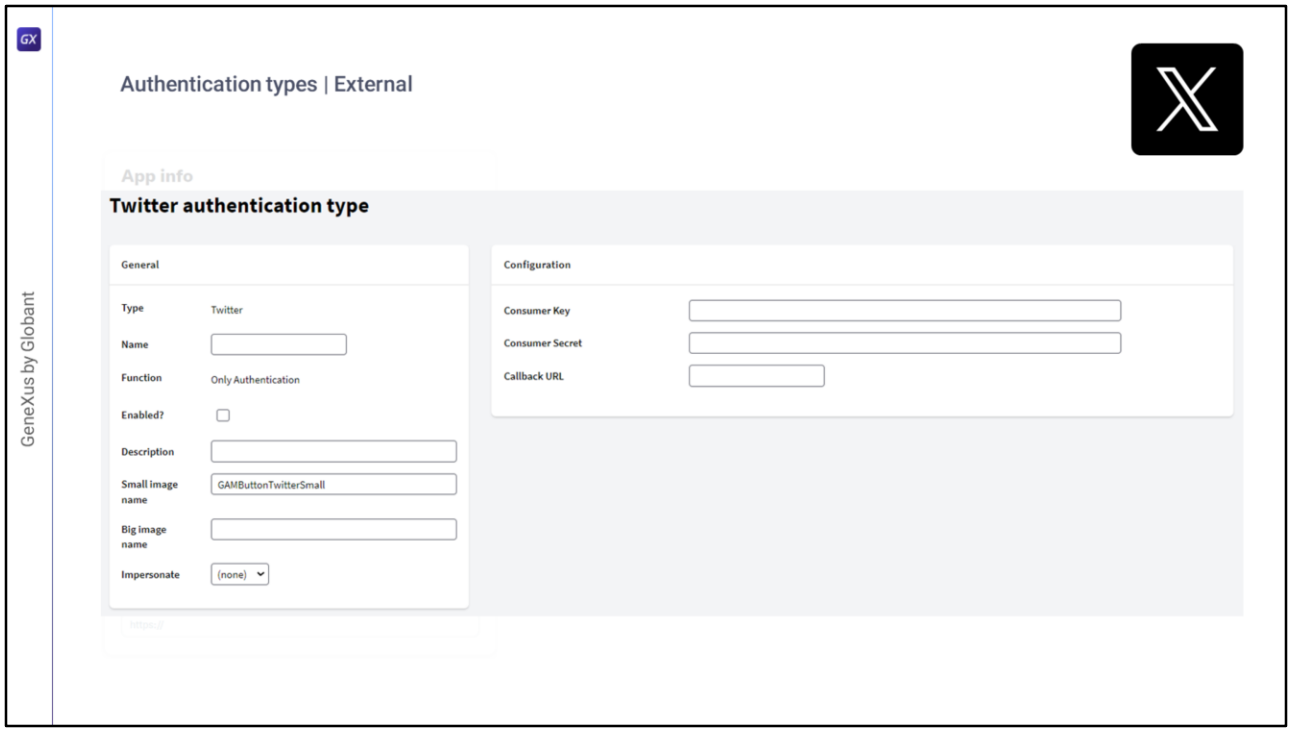


Em segundo lugar temos o Facebook.

Neste tipo, devem ser seguidas duas etapas:
Em primeiro lugar deve ser criada uma "aplicação de cliente de Facebook" em seu site e obter um ID e chave (denominada "Segredo") para sua aplicação.
Em segundo lugar, deve ser definido o "Tipo de autenticação do Facebook" no backend ou API do GAM.

Realizando estas etapas detalhadamente, já está configurado o tipo de autenticação corretamente.

Este tipo pode ser usado em aplicações web e aplicações móveis nativas e por trás se resolve mediante Oauth 2.0.

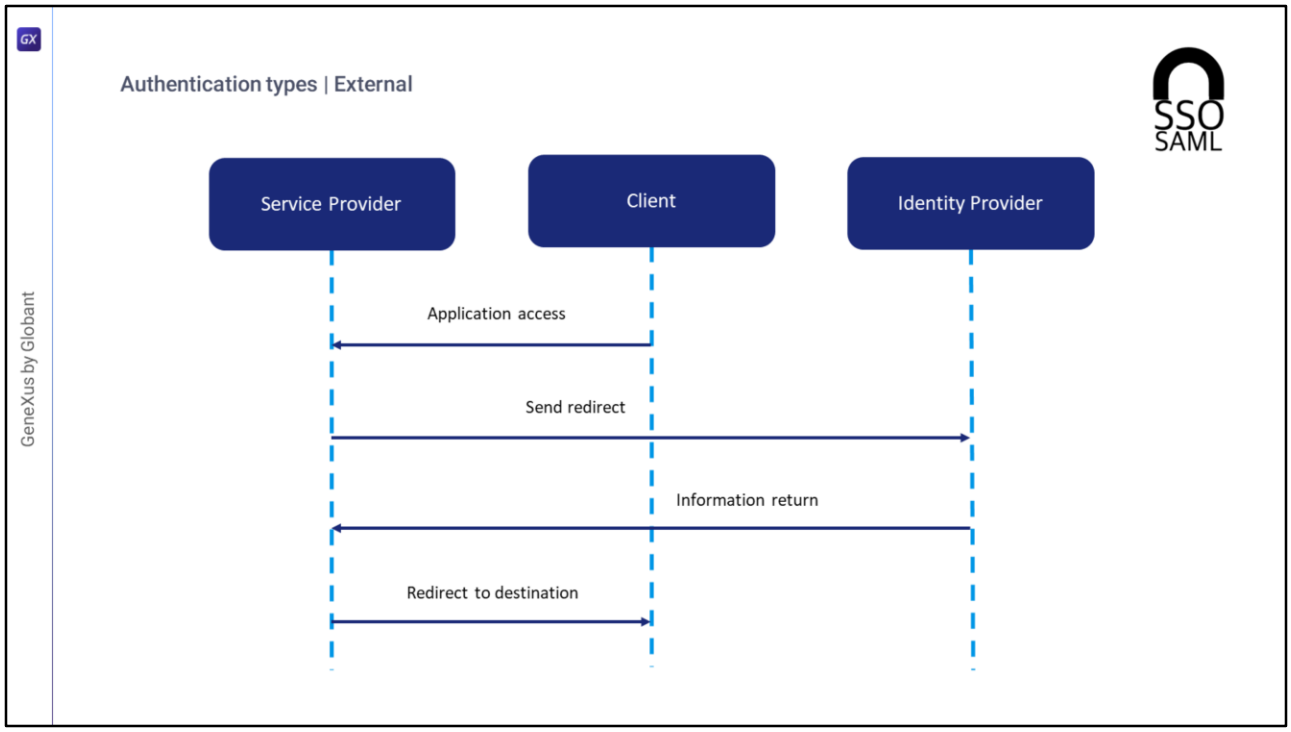


Depois temos o Twitter.

Este caso é executado da mesma forma que o Facebook.
Como etapa 1, deve ser criada uma aplicação do Twitter em seu site e obter a chave e segredo do consumidor para essa aplicação.
Como etapa 2, é definido o tipo de autenticação do Twitter utilizando o backend GAM.

Novamente, como no Facebook, este tipo de autenticação pode ser utilizado em aplicações web e também em aplicações móveis nativas.

Na Wiki de GeneXus podem ser encontrados com detalhes este e todos os tipos de autenticação existentes para GAM.

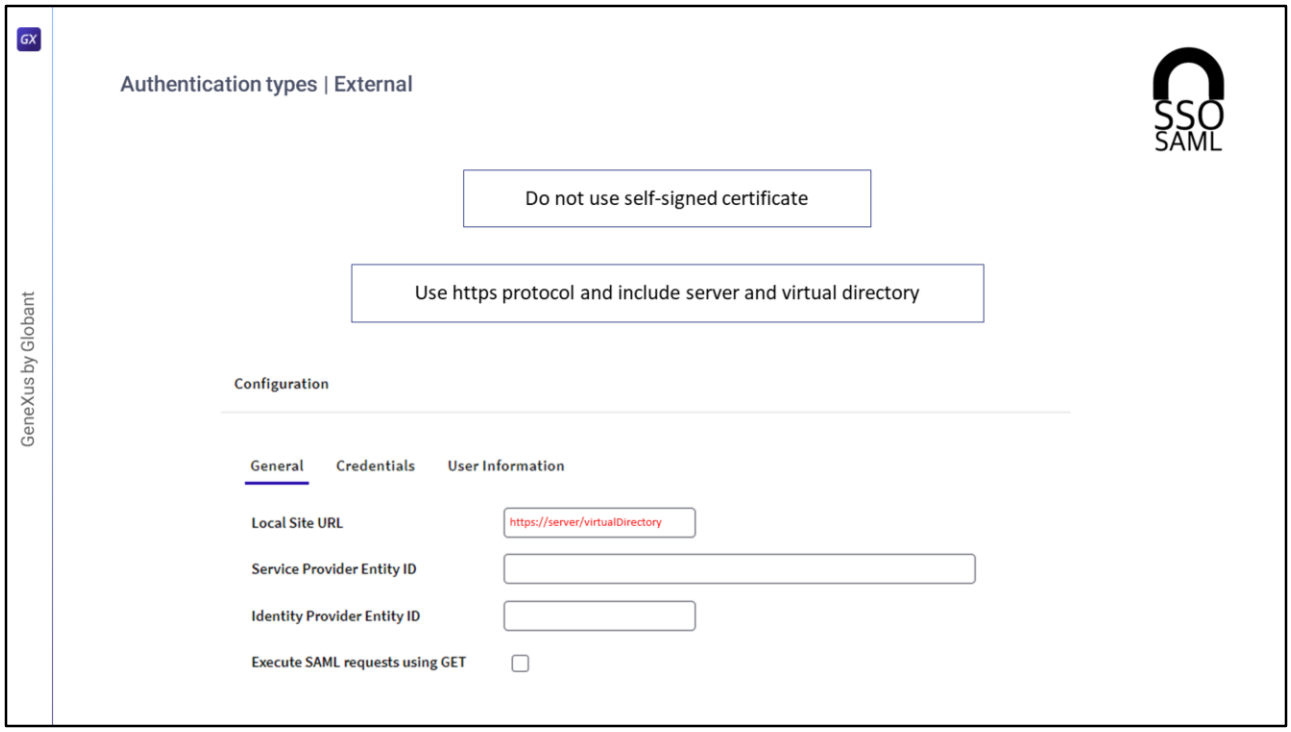


GAM permite autenticação utilizando qualquer provedor SAML em versão 2.0.

SAML é um mecanismo de comunicação seguro baseado em XML para comunicar identidades entre organizações.

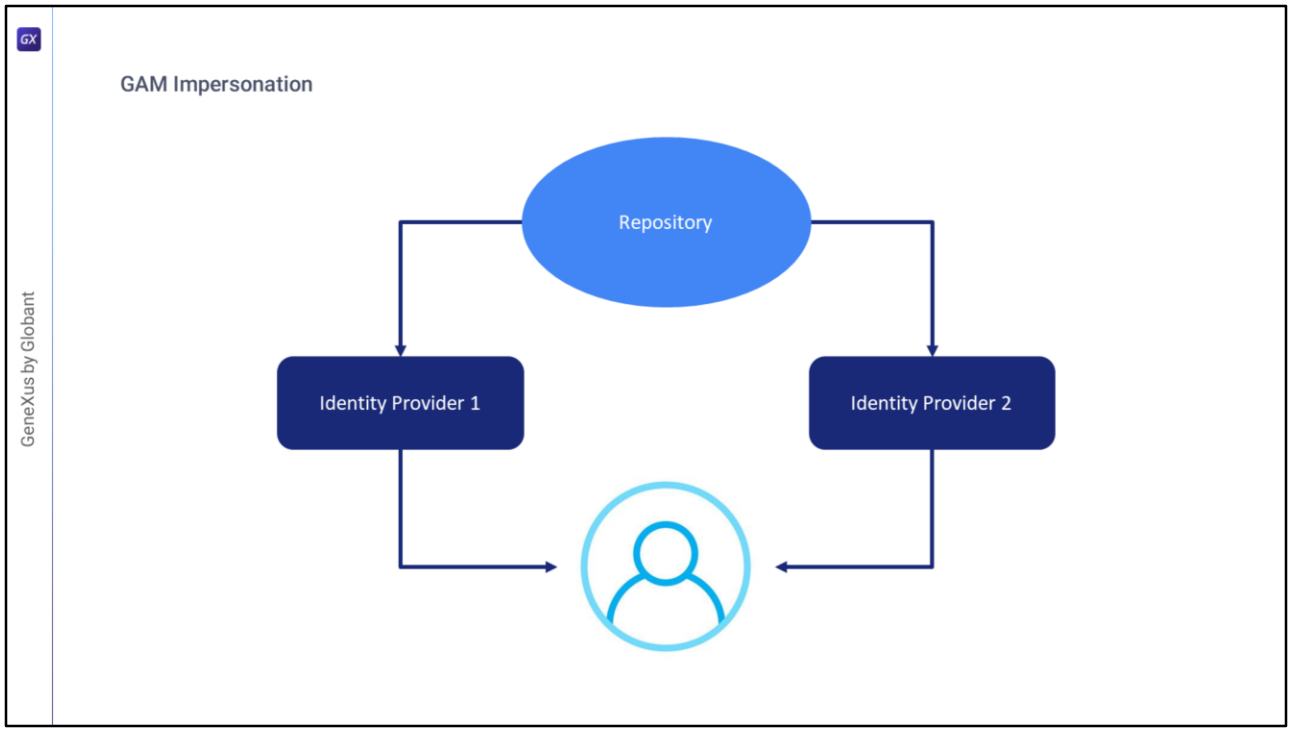
Um dos casos de uso que resolve SAML também é SSO, por isso evita a necessidade de manter várias credenciais em vários locais e aumenta a segurança ao mesmo tempo que reduz as tarefas de tempo de administração.

Em SAML participam duas entidades além do cliente: um provedor de serviços e um provedor de identidade.
Um fluxo de início de sessão é realizado, de modo geral, da seguinte forma:
Em primeiro lugar o usuário tenta acessar uma aplicação hospedada em um provedor de serviços.
Este Provedor gera uma solicitação de autenticação e a envia através de um redirecionamento ao navegador do usuário.
O provedor de identidade recebe a solicitação, autentica o usuário solicitando credenciais de acesso válidas ou comprovando que existem cookies de sessão corretos, e gera a resposta a ser retornada ao navegador do usuário.
Finalmente, o usuário é redirecionado para a URL de destino.



Algo a ser mencionado em SAML é o seguinte:

- Em relação aos certificados, o recomendável é não usar certificados autoassinados.
- A propriedade Local Site URL deve ter protocolo https e incluir server e diretório virtual como vemos em tela.



Quando o Repositório do GAM permite que os usuários finais se autentiquem com diferentes provedores de identidade, de forma predeterminada, são atribuídos a diferentes Usuários do GAM. Por motivos de segurança, os usuários podem ser autenticados
utilizando diferentes mecanismos dependendo da fonte de acesso utilizada. No entanto, a informação de início de sessão deve ser atribuída ao mesmo usuário lógico do GAM.

A Representação (Impersonation) permite que o repositório tenha dois mecanismos de autenticação diferentes mas que convergem para o mesmo usuário.
Isto é útil para casos, por exemplo, nos quais não é possível utilizar o mesmo tipo de autenticação a partir da intranet e a partir da internet, mas é desejado que o usuário seja o mesmo.
Também é utilizado quando é desejado migrar de um tipo de autenticação para outro, onde nesse caso o tipo de autenticação "representada" é aquele que está sendo migrado.

Conforme o tipo de autenticação, existem diferentes critérios para mapear usuários, que estão detalhados na Wiki de GeneXus.

Para fechar este tema, no vídeo seguinte passaremos para uma série de demonstrações com a finalidade de mostrar os casos de forma prática com mais detalhes.


GeneXus by Globant
GeneXus™
by Globant
training.genexus.com