O processo de autenticação entre duas aplicações geralmente envolve a verificação da identidade do usuário ou da aplicação solicitante. Abaixo está descrito em passos um exemplo de processo de autenticação comumente utilizado, chamado de autenticação baseada em tokens:

1. O usuário ou a aplicação solicita acesso à aplicação de destino. Isso pode ser feito por meio de um formulário de login, uma solicitação de API ou outro meio de comunicação.
2. A aplicação de destino recebe a solicitação de acesso e verifica as credenciais fornecidas pelo usuário ou aplicação solicitante. Isso pode envolver a verificação do nome de usuário e senha, a autenticação de chave de API ou outras informações de identificação.
3. Se as credenciais estiverem corretas, a aplicação de destino gera um token de autenticação. Esse token é um objeto estruturado que contém informações sobre a identidade do usuário ou da aplicação e pode incluir permissões, tempo de expiração e outras informações relevantes.
4. O token de autenticação é retornado para o usuário ou a aplicação solicitante. Normalmente, ele é armazenado localmente para uso posterior.
5. Em solicitações subsequentes, o token de autenticação é incluído nas requisições. Isso pode ser feito através de cabeçalhos HTTP, cookies ou outros mecanismos de transporte de dados.
6. A aplicação de destino verifica a validade do token de autenticação recebido. Isso envolve a verificação da assinatura do token, a validação do tempo de expiração e outras verificações de segurança.
7. Se o token de autenticação for válido, a aplicação de destino considera o usuário ou a aplicação autenticada e permite o acesso aos recursos ou funcionalidades solicitados. Caso contrário, é retornada uma resposta de erro ou o acesso é negado.