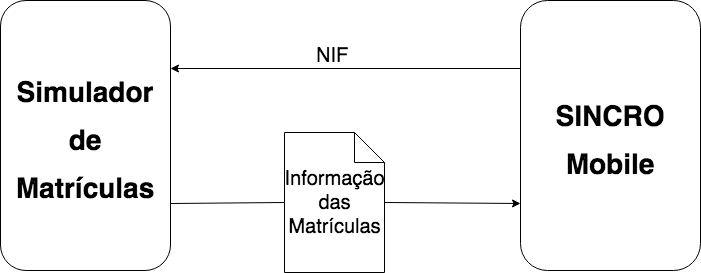
Verificação da matrícula

# Implementação

No âmbito do projeto, de forma a cumprir as funcionalidades apresentadas, vai ser indispensável trabalhar com informação privada dos Cidadãos, mais propriamente a informação referente às matrículas. Dado que não nos é permitido acesso à informação foi necessário a conceção de um sistema simulador de matrículas.



O sistema efetuado para simular a obtenção da informação das matrículas tem como arquitetura a figura acima apresentada.

O SINCRO Mobile irá comunicar diretamente com o simulador, fazendo um pedido ao mesmo com o NIF do qual pretende ter acesso à informação das matrículas. Ao ser feita a confirmação do NIF o Simulador de Matrículas irá enviar a informação de todas as matrículas presentes registadas em nome do Cidadão com o respetivo NIF enviado. As matrículas disponibilizadas pelo simulador são registadas previamente possibilitando a simulação desta operação.

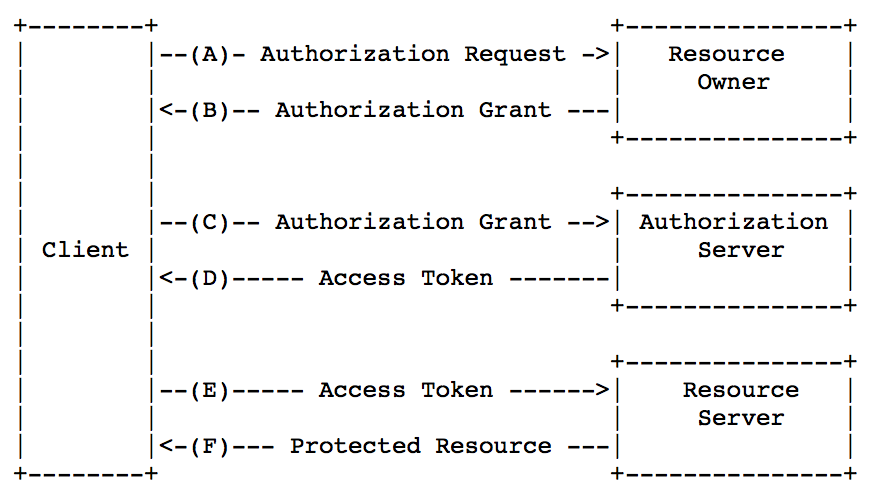
# Problemas e Solução

Esta forma de obtenção de informação privada não será a mais correta, uma vez que não existe nenhuma preocupação quanto à segurança durante o processo de troca de dados entre os dois sistemas informáticos.

O Simulador de Matrículas deverá utilizar uma entidade externa para registo de novas entidades que pretendam e sejam autorizadas pelo simulador a tal informação. Através desta arquitetura deverá ser possível a autenticação dos sistemas previamente registados de forma a lhes ser garantido o acesso à informação reservada. Por sua vez, favorecendo a segurança do Simulador de Matrículas para acessos indesejados de entidades maliciosas.

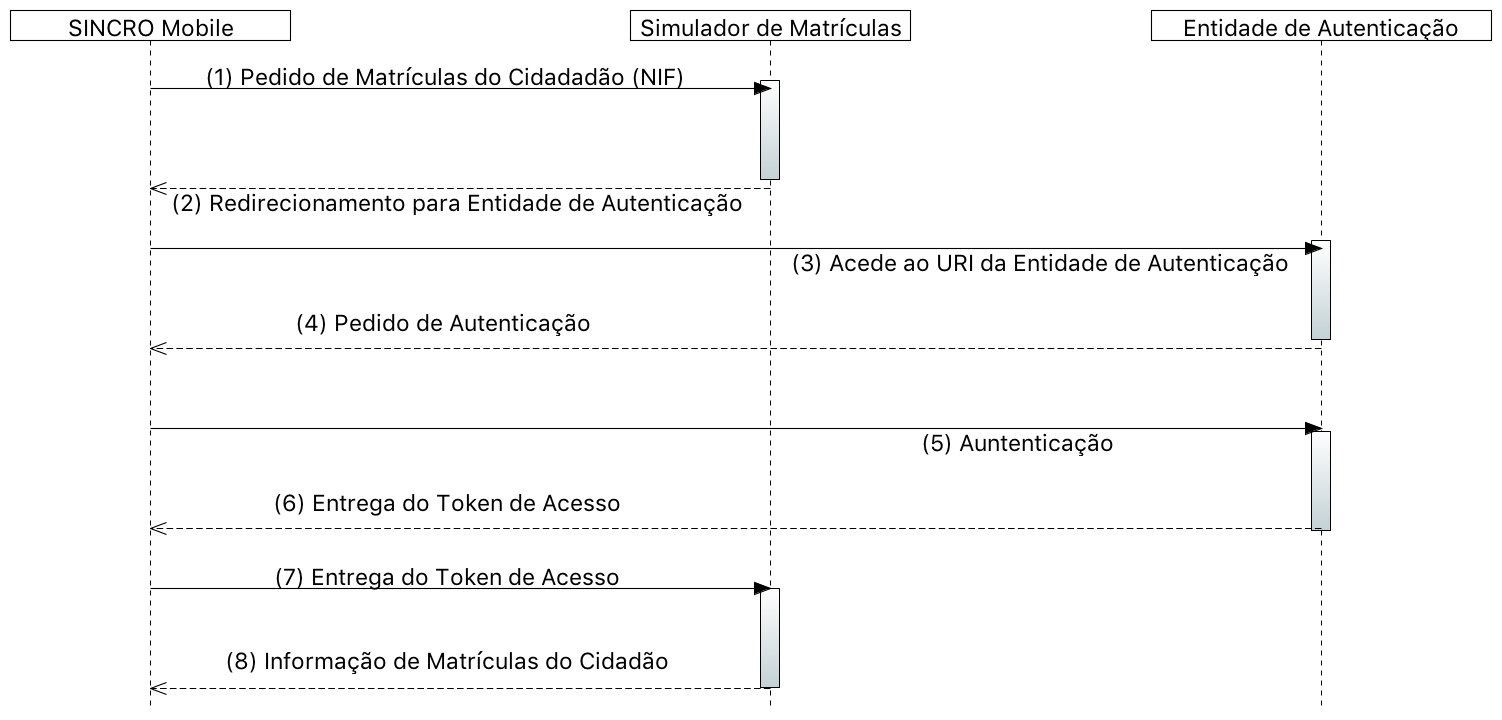
# Atual Processo de Autorização a Recursos Privados.

Com base na solução procurada para realizar a autorização no acesso a recursos privados, existe uma tecnologia de autorização que permite o acesso limitado por aplicações exteriores via HTTP. A tecnologia dá pelo nome de OAuth 2.0 e o seu foco principal é a simplicidade e promover fluxos específicos de autorização para aplicações web, desktop, entre outros. Na figura abaixo é possível verificar o fluxo de comunicação entre os diferentes participantes de forma a garantir uma correta autorização de recursos privados.



# Aplicação do Fluxo de Autorização a Recursos Privados

De forma a simplificar o funcionamento da tecnologia de autorização anteriormente falado, OAuth 2.0, decidimos conceber um diagrama de sequência mais próximo do objetivo principal deste capítulo. Os participantes do diagrama proposto são o SINCRO Mobile (Client), Simulador de Matrículas (Resource Owner/Server) e a Entidade de Autenticação (Authorization Server).



Fluxo de Comunicação entre Participantes:

1. É enviado o NIF para o Simulador de Matrículas de forma a este saber quais as informações de matrículas que deve entregar como resposta do pedido.
2. Uma vez não autorizado, SINCRO Mobile é redirecionado para a Entidade de Autenticação. Nesta resposta é enviado juntamente um Grant de Autorização.
3. Acede ao URI da Entidade de Autenticação onde entrega o Grant de Autorização. Com base no Grant de Autorização a Entidade de Autenticação saberá a qual entidade o SINCRO Mobile pretende ter autorização de dados, neste caso trata-se do Simulador de Matrículas.
4. É devolvido ao SINCRO Mobile um formulário de autenticação.
5. É submetido o formulário de autenticação com os dados de autenticação do SINCRO Mobile.
6. É entregue ao SINCRO Mobile um Token de Acesso para os recursos privados.
7. O Token anteriormente recebido no passo (6) é reenviado ao Simulador de Matrículas que irá verificar a validade e autenticidade do mesmo.
8. Finalmente é entregue em caso de sucesso do passo (7) a informação das matrículas do NIF enviado no passo (1).